MITEL BORDER GATEWAY Release 8.0
ENGINEERING GUIDELINES

MITEL®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

Mitel is a trademark of Mitel Networks Corporation.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

MBG - Engineering Guidelines
DK121047
Release 8.0
June 7, 2013

®,™ Trademark of Mitel Networks Corporation
© Copyright 2011, Mitel Networks Corporation
All rights reserved

CONTENTS

About this Document 1
Overview 1
Prerequisites 1
About the MBG Documentation Set 1
Supported Configurations 2
Services 2
Teleworkers and Remote Offices 2
Overview 2
Mitel Border Gateway as Internet Gateway 3
Additional Local Networks 4
Mitel Border Gateway in a DMZ 5
NAT Traversal for MICD 6
Secure Gateway for Broadview Networks silhouette HKS 6
Secure Recording Environment 7
MBG Deployed on the LAN for Call Recording 7
SIP Trunking 10
Daisy-Chain Deployments 11
Special IT Policy Deployment 11
Reduced Bandwidth for Remote Sites 12
MBG in MAS 13
MAS on the LAN 13
MAS on the Network Edge 13
MBG in vUCC 14
Partial Service Configurations 14
Common Requirements 15
Supported ICP Versions 15
Administrative Access 15
Firewalls (DMZ deployment) 15
Known Issues 16
Checkpoint “NG” Firewalls 16
Port-Forwarding Firewalls 16
SIP-Aware Firewalls 16
UDP Flood Protection 16
Firewall Configuration Common to all Services 17
Remote Phone Access 18
Remote Site Requirements 18
Router 18
VPN Connectivity 19
Using an Existing VPN 19
Corporate Firewall & Network Configuration for VPN Access 19
Bandwidth Requirements for the Remote Site 19
Configuring the Remote Site Firewall 21
TFTP Behavior 22
Firewall Configuration for Remote MiNet Devices 22
Configuring MBG for Remote SIP Devices 23
Remote SIP Device Limitations 23
Tuning Global Parameters 23
DNS Support 23
Firewall Configuration for Remote SIP Devices 23
SIP Trunking 25
Overview 25
Bandwidth Requirements 25
Resilient Trunk Configuration 25

DNS Support....26
Firewall Configuration for SIP Trunking....26
Call Recording....27
Call recording vs. Local streaming....27
Indirect Call Recording....27
Additional Application Requirements....28
Unified Communicator Advanced (UCA) v4.0+....28
Mitel Contact Center....28
Web Proxy....29
Special consideration for MCA through Web Proxy....29
Remote Management Service....29
Additional Security Considerations....30
SIP Security....30
Traffic Shaping....31
Overview....31
Technical Details....31
Clustering....33
Overview....33
Cluster Zones....33
Node Weighting....34
Additional Considerations....35
Firewall Configuration for Clustering....35
Advanced Options....36
Resiliency....36
IP Translations....36
Streaming Addresses....37
DMZ Deployment Profile....37
Gateway Deployment Profile....37
RTP Frame Size....37
TFTP Block Size....38
Set-side Codec....38
SRTP Port Range....38
DSCP....38
Sizing Your Installation....40
Determining Line Size for Large Sites....40
Step One: Determine Call Rate....40
Step Two: Determine Service Rate....40
Step Three: Determine Grade of Service....40
Step Four: Erlang-B Calculator....41
Determine Call Equivalents....41
Determine Bandwidth Requirements....41
G.711 Calculation....42
G.729a Calculation....42
Video Calculation....43
Fax Calculation....44
Call Recording Calculation....44
Example Bandwidth Calculation....44
Hardware Selection....45
Performance Characteristics and Limits....45
Physical Hardware....45
VMWare Virtual Hardware....46
Web Proxy and Remote Management Service Requirements....46
UCA and MCA Requirements....46
Mitel Contact Center Softphone Requirements....47
Virtual MBG Considerations....49

Licensing....49
Upgrades....49
Host Server Requirements....49
Hardware....49
Software....50
High-Availability....50
Solutions To Common Problems....51
Changing a Cluster Node's IP Address....51
T.38 Faxing Does Not Work With NAT....51
Appendix A: Firewall Configuration Reference....52

1 About this Document

1.1 Overview

The purpose of this document is to describe configuration rules, provisioning, and performance information for the Mitel Border Gateway, and associated products in order to assist in sales and support of this product. This information is intended for Training, Sales and Product support staff and complements other sales material and product documentation.

Note: The Secure Recording Connector (SRC) has been consolidated into MBG. Accordingly, although this document discusses the SRC control interface and its protocol, it does not treat the SRC as a separate feature.

1.2 Prerequisites

The Mitel Border Gateway application runs on the Mitel Standard Linux (MSL) Server. The reader should first become familiar with the *MSL Installation and Administration Guide* and the *MSL Qualified Hardware* document. These are available from http://edocs.mitel.com.

1.3 About the MBG Documentation Set

Mitel documentation is available from http://edocs.mitel.com. (Note: a Mitel On-Line account is required to access eDocs.) The following guides provide complete information about MBG:

- The *MBG Engineering Guidelines* (this document).
- The *Mitel Border Gateway Blade Installation and Maintenance Guide* provides information about system requirements, installation of MBG, and configuration of MBG options and firewalls.
- The *Mitel Border Gateway Online Help* provides information about MBG configuration and maintenance.
- The *Remote IP Phones Configuration Guide* provides information about configuring remote phones.

2 Supported Configurations

2.1 Services

MBG provides the following services:

- **Remote MiNet IP Phones** The classic use of MBG, formerly known as the Teleworker Solution, permits remote MiNet phones to securely access the corporate phone network over the Internet.
- **Remote SIP IP Phones** Permits Teleworker functionality for SIP hard or soft phones over the Internet.
- **SIP Trunking** Allows a corporate phone switch to connect SIP trunks to a SIP trunk provider, protecting the switch from malformed messages, unauthorized use, and various attacks, and providing an anchor point for media streams.
- **Call Recording** Formerly the Secure Recording Connector, this service allows secure recording of phone calls by a third-party application

In addition, the MBG server can host the **Remote Proxy Services** blade to provide the following services:

- **Web Proxy: end-user access from the WAN to applications hosted inside the firewall**
- **Remote Management Service:** administrative access from the WAN to applications hosted inside the firewall

Please refer to the Remote Proxy Services documentation for details.

MBG can be deployed in several ways depending on the services required.

2.2 Teleworkers and Remote Offices

Overview

The original design intent of MBG is to provide a Teleworker solution. Once an MBG server is installed, extensions from the office PBX can be extended across the Internet to permit MiNet phones to work from homes, remote offices, hotels, etc.

In this use-case, either the server-gateway profile or DMZ profile could be used depending where on the network MBG is to be deployed. If deploying behind an existing firewall on a DMZ, then a single network interface and DMZ profile is appropriate. If deploying beside an existing firewall, or if there is no existing firewall, then server-gateway profile is appropriate.

Failure to follow these guidelines will result in one-way or no-way audio.

Warning: Some firewalls which use port-forwarding to simulate a DMZ are *Port-forwarding Firewalls*. See the Common Requirements chapter for full details.

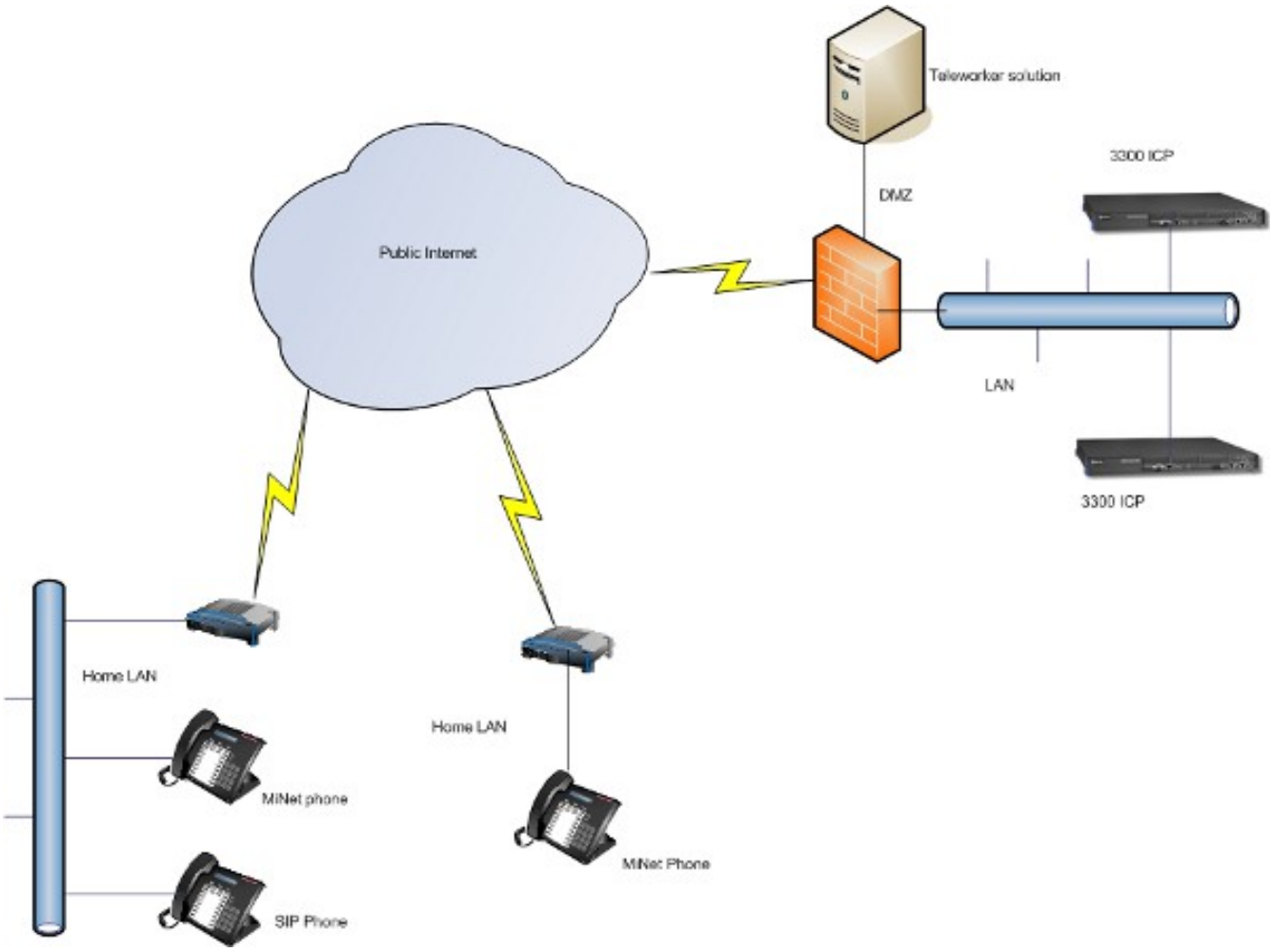


Figure 1: MBG in traditional Teleworker configuration

Mitel Border Gateway as Internet Gateway

Mitel recommends deploying the Mitel Standard Linux server with Mitel Border Gateway as the Internet gateway and firewall for any enterprise without an existing firewall. Figure 2 shows a example of this configuration using the Mitel Border Gateway and a Mitel Communications Director (3300 ICP).

MBG requires two network interfaces and two addresses for this configuration. The external address must:

1. Be a static address that does not change
2. Be directly attached to a NIC on the MSL server
3. Be reachable from the public network/Internet
4. Be reachable from the internal network/LAN
5. Not be subject to NAT or behind another firewall

The interface may be configured via DHCP, PPPoA, PPPoE or similar technology, but the address it receives must always be the same.

Warning: If the external address changes, all teleworker phones must be reprogrammed with the new address.

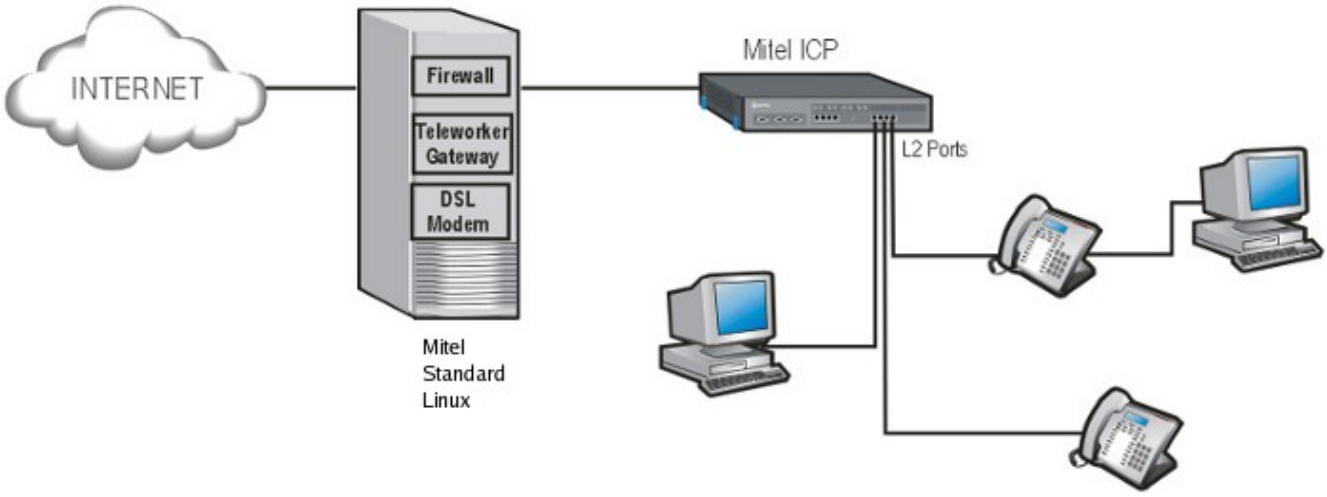


Figure 2: MBG as Internet Gateway (no enterprise firewall)

An enterprise can take advantage of the DSL, authenticated DHCP and PPPoE/PPPoA[1] capabilities of the MSL server. MSL additionally provides NAT for all devices at the enterprise, a stateful packet filter firewall, and optional port-forwarding.

Note: If desired and if hardware is available, a third interface may be configured in MSL. This interface might be useful as a dedicated interface for clustering if a network between the MBG servers can be set aside for this purpose.
Alternatively, the third interface could be put into bridged mode on MSL 9.2+ to permit an MBG server in parallel with an existing firewall to transparently handle all traffic from that firewall and accomplish traffic shaping. See *Traffic Shaping* for full details.

Additional Local Networks

Additional internal networks or subnets that require access to the Mitel Border Gateway can be added via the *Local Networks* panel of the server manager. This access can be limited to individual hosts, or large network blocks can be used. In all cases, the *Router* property should be set to the address of the router on the subnet attached to the MSL server's internal interface.

For example, to allow access from the single subnet 192.168.12.0/24, you would enter a network of 192.168.12.0 and a mask of 255.255.255.0 in the *Local Networks* panel, plus the address of the router on the local subnet through which this network can be reached.

If the customer's network has multiple subnets with a common prefix, access can be allowed from the prefix. For example, if the customer uses various subnets within the 192.168.0.0/16 network, enter a network of 192.168.0.0 and mask of 255.255.0.0 in the *Local Networks* panel, and allow the local router to determine the routing to the individual subnets.

1 Limited support is provided for PPoA. Mitel recommends the use of a D-Link DSL 300T modem at the enterprise site if PPPoA connectivity is required in gateway mode. Configure the modem to provide DHCP on the internal interface, and use DHCP on the MSL server to configure the public interface. The modem acts as a bridge. Note that PPPoA routers that provide NAT will not work here.

Warning: The local networks configuration serves as both application access control and as static routing configuration.

Note: *Local Networks* is a feature of MSL. Refer to the MSL documentation for a full description of its capabilities.

Mitel Border Gateway in a DMZ

The Mitel Border Gateway can also be deployed behind a customer-provided or customer-managed firewall as shown in Figure 3. This firewall *must* have 3 network interfaces (ports): WAN, LAN, and DMZ. Two-port firewalls are *not supported.* It should also be noted that some “DSL routers” with “DMZ” port forwarding are simply two-port NAT devices and should be treated as any other two-port firewall. Deployment of the Mitel Border Gateway behind such devices is not supported.

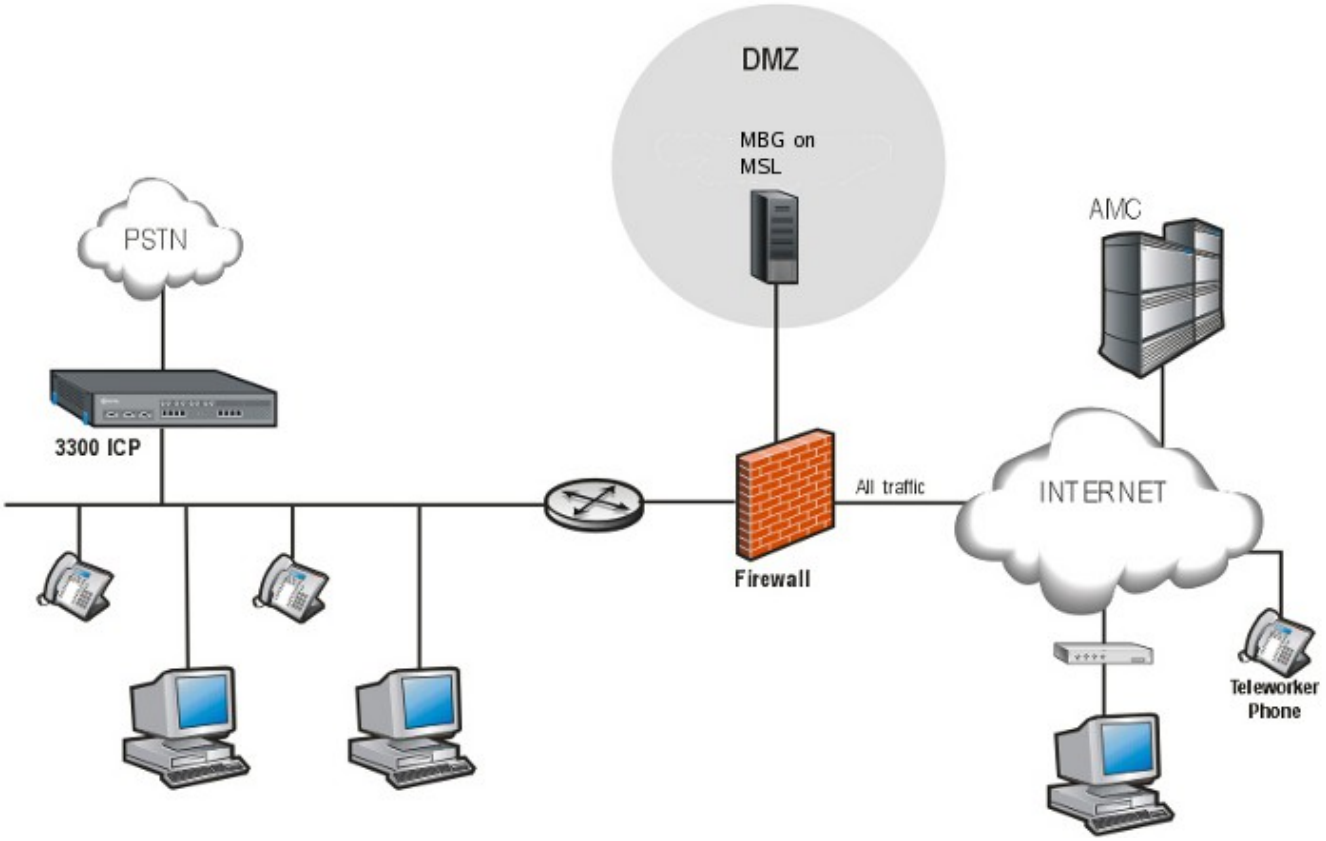


Figure 3: MBG deployed in a DMZ

MBG requires one network interface and two addresses for this configuration. The interface must be configured with a static address allocated from the DMZ network range. This is typically an RFC 1918 “private” address. The enterprise firewall must be configured with an address allocated from the public/Internet range. This address must be:

1. reachable from the public network/Internet
2. reachable from the internal network/LAN

3. able to reach the internal network/LAN
4. preferably dedicated solely to MBG, but also see *Port-forwarding firewalls*

2.3 NAT Traversal for MICD

In a multi-tenant MICD install, it is possible to find tenant sites with overlapped network ranges, and without NAT at the customer edge network. In this case, MBG can be used to perform NAT traversal between the tenant sets and the MICD solution.

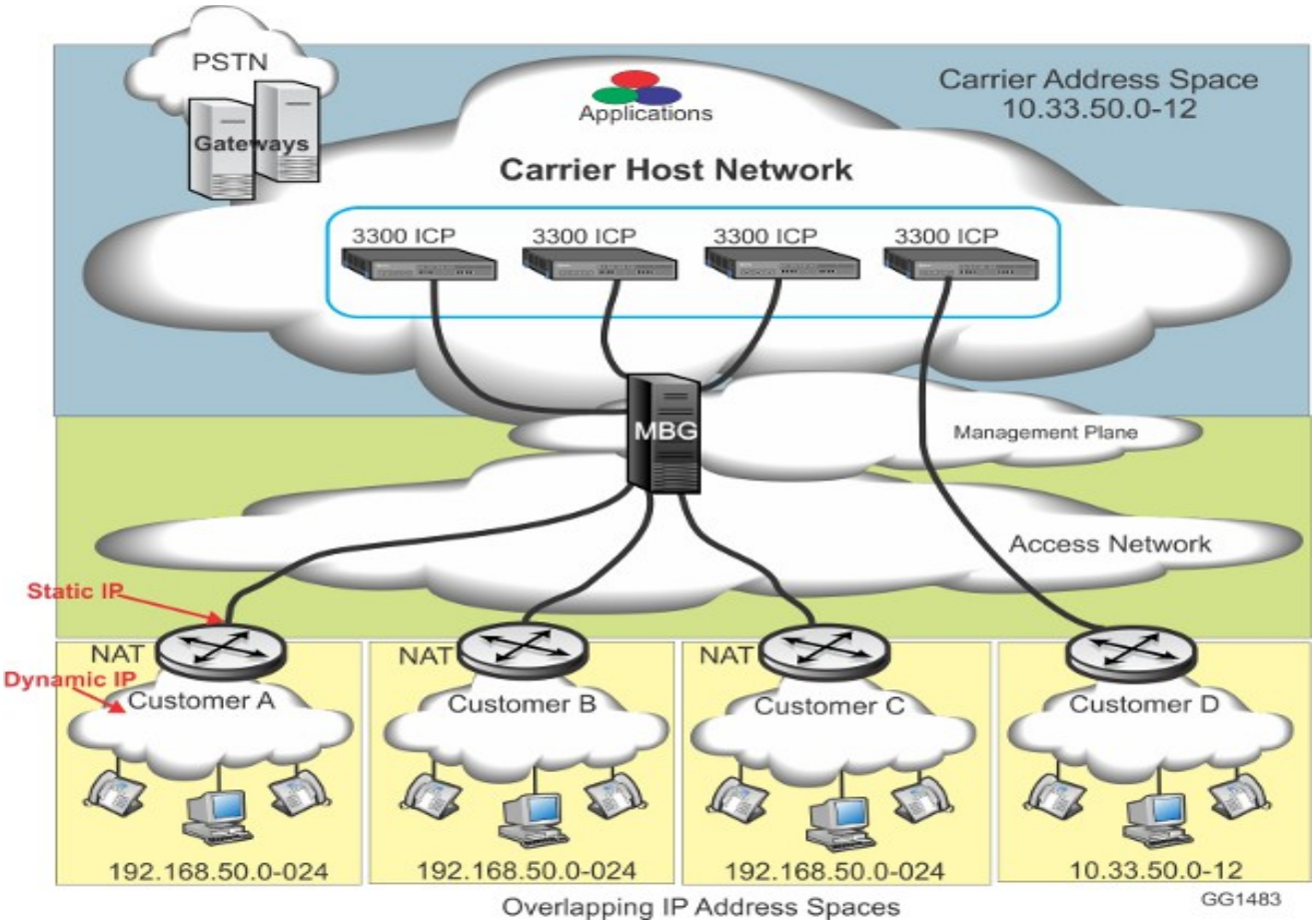


Figure 4: MBG providing NAT traversal for MICD

2.4 Secure Gateway for Broadview Networks silhouette HKS

The Broadview Networks hosted key system provides service to various tenants across leased lines, MPLS circuits, or the Internet from a common carrier. Customers are provided with either MiNet or SIP sets, and the MBG acts as a Session Border Controller for both protocols. DNs are unique within each tenant but may overlap between tenants.

Note: Please contact Broadview Networks to determine which MBG versions are compatible with silhouette, and for all support inquiries.

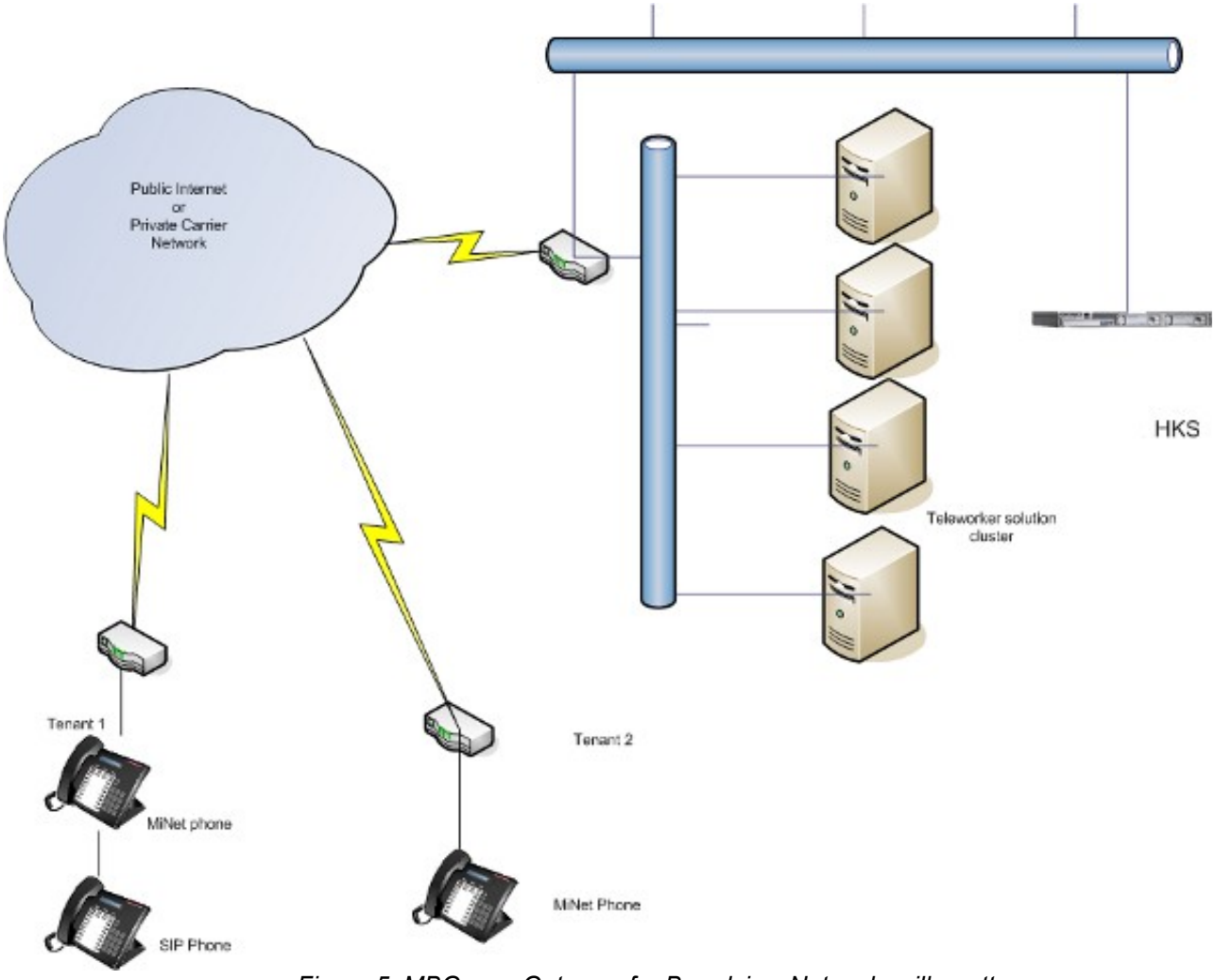


Figure 5: MBG as a Gateway for Broadview Networks silhouette

2.5 Secure Recording Environment

When MBG is provisioned with call recording licenses, it can provide a secure man-in-the-middle for call recording. This mode is supported only in a LAN environment.

It is advisable to disable MiNet restrictions on the MBG server providing call recording service, as having all LAN sets authenticate through MBG is likely not required.

Teleworker sets connected through an MBG at the network edge can be recorded as well, by configuring the edge MBG such that the desired sets point to the LAN MBG as if it was an ICP.

MBG Deployed on the LAN for Call Recording

When possible, Mitel recommends deploying the MBG call recording server on the same LAN segment as the ICP(s) with which it will be working. However, it is often practical to use a separate segment if not all devices should be recordable.

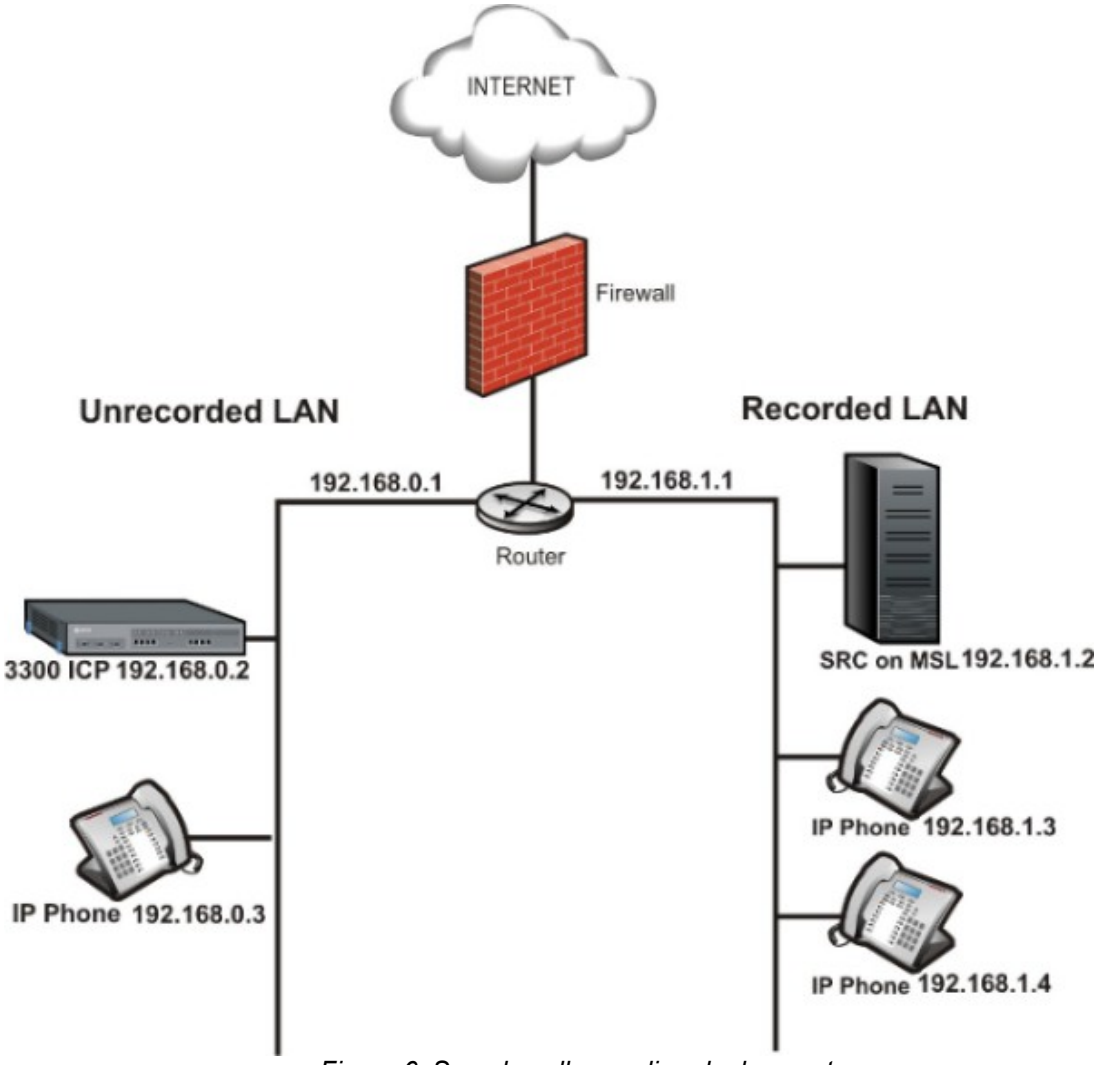


Figure 6: Sample call recording deployment

Figure 6 shows one sample configuration that could be used. IP phones that are to be recorded are on the same LAN segment as the MBG server. DHCP is enabled in MSL, and MBG provides DHCP configuration such that the sets use the MBG server as their TFTP server and as their ICP. MBG then proxies the set registrations to the real ICP on the other segment. Sets on a different LAN segment using the MCD DHCP server connect directly to the MCD and are therefore not recordable.

As an alternative to changing the network topology, each set that should be recordable can be individually programmed to connect to the MBG. Hold down the “7” key and put each set into Teleworker mode. At the prompt, enter the IP address of the MBG.

MBG servers can be chained together to allow recording of remote teleworker phones. Figure 7 below shows an example of a teleworker set connecting through the edge MBG to an MBG server for call recording (and finally to the MCD), so that it can be recorded along with the sets on the Recorded LAN. To configure this scenario, an “ICP” entry is added to the edge MBG containing the IP address of the LAN MBG used for recording. All remote sets that should be recordable must be configured with that “ICP”. The recording MBG will then proxy the remote sets to their real ICP.

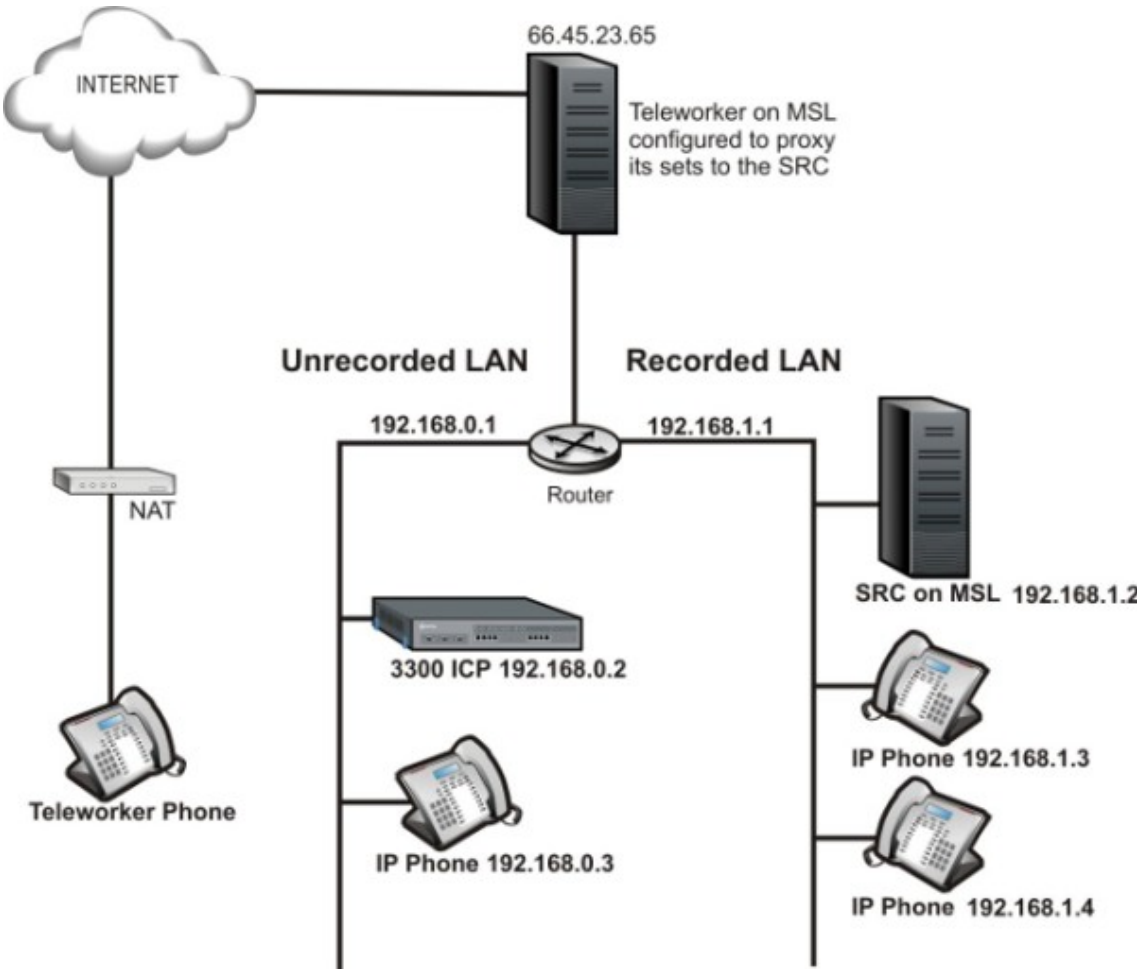


Figure 7: Recording teleworker sets

Note: CIS softphone (Contact Center) can function properly in this configuration. However, only the signaling and voice should be proxied through the call recording MBG. Additional applications protocols should be proxied directly from the edge MBG to the CIS server.

Warning: This is the only supported way to have both teleworker sets and call recording of LAN sets. Combining teleworker service and call recording of LAN sets on a single server is not supported.

2.6 SIP Trunking

MBG introduced support for SIP trunks in release 5.1. The SIP trunk is established from the MCD to the SIP trunk provider, using MBG as a SIP-aware firewall and proxy, as shown in Figure 8 below. MBG's SIP trunk service provides:

- NAT traversal of media and signaling
- Media anchoring for the remote provider, regardless of the internal device
- SIP adaptation and normalization to improve interoperability
- Protection from malformed & malicious requests, various types of attack, and request flooding

When providing SIP trunk service, MBG can be deployed either in the DMZ of, in parallel with, or in place of an existing firewall.

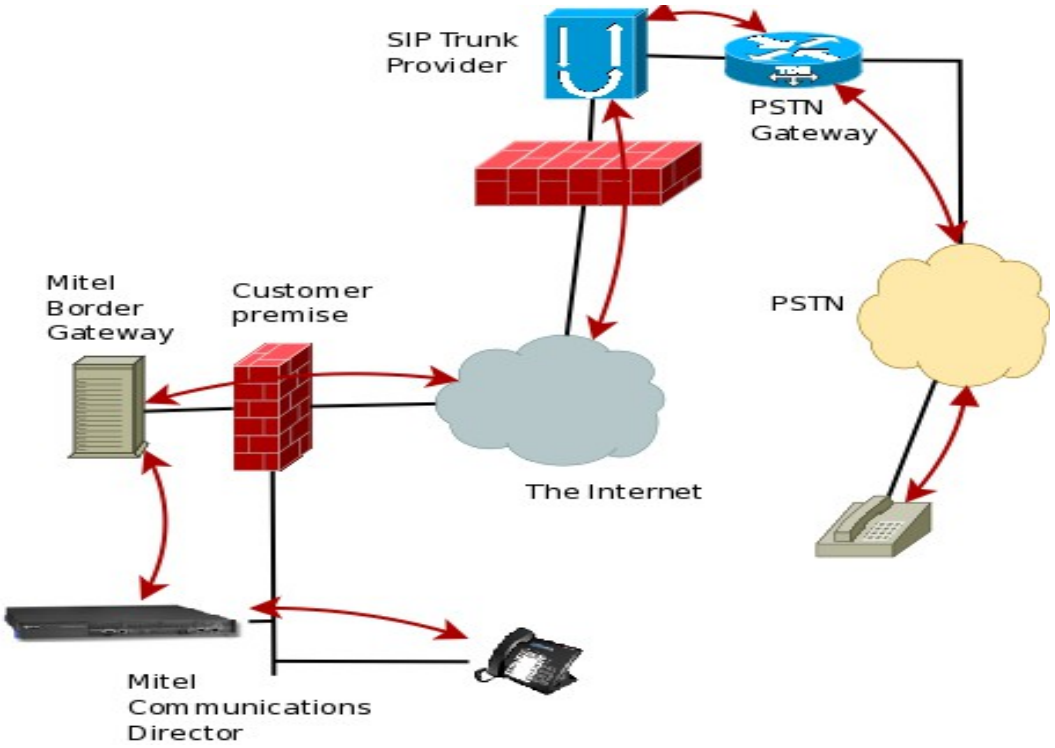


Figure 8: MBG as a SIP Trunk Proxy

Some of the key benefits of using SIP trunks are:

- consolidation of capacity; all trunks come to one location, calls routed to branch offices over MPLS or VPN links already in place
- increased simplicity for bandwidth management
- local phone numbers from anywhere in the world to permit customers to reach the company in question easily
- cheaper toll-free service in most cases
- cost savings over PRI/T1/POTS lines

- increased resiliency with the potential for disaster recovery configuration

2.7 Daisy-Chain Deployments

"Daisy-chaining" is a technique of pointing one MBG at another that can work around certain bandwidth and routing restrictions. The servers are configured such that all traffic between the sets and ICPs traverses all MBG servers in series, like following links in a chain.

A "daisy-chained" MBG is one that is configured to accept all incoming requests (authentication is disabled) and pass them "upstream" to another MBG, where the standard authentication is performed.

Note: In this context, "upstream" refers to the direction approaching the ICP on the LAN.

Warning: Daisy-chaining is only supported for MiNet and SIP phones. SIP trunking and remote applications have not been formally tested with MBG daisy-chain deployments.

The two main applications of daisy-chaining are to comply with certain IT deployment policies and to reduce bandwidth for remote sites.

Special IT Policy Deployment

Daisy-chaining the DMZ MBG server to a LAN MBG server minimizes the scope of the firewall rules required to facilitate communications between them. The firewall administrator can permit traffic only between those two servers instead of across the entire LAN where sets may be located.

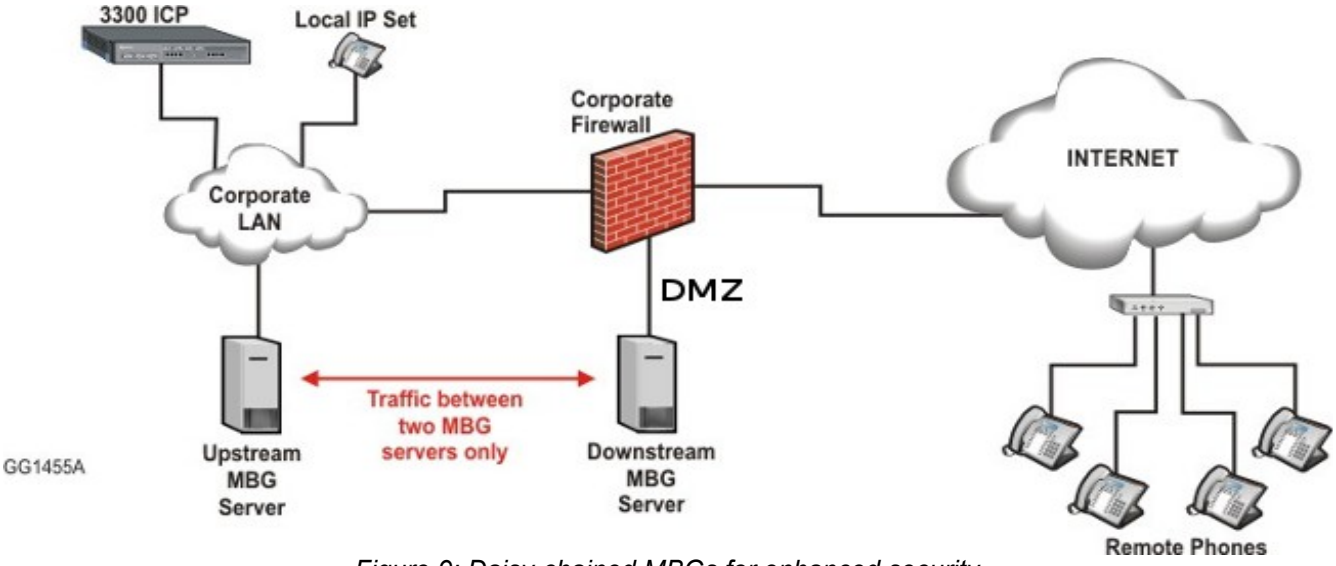


Figure 9: Daisy-chained MBGs for enhanced security

This configuration places the downstream server in the DMZ and the upstream server on the LAN. The servers should use the network profiles of DMZ mode and LAN mode, respectively.

Note: Authentication should be disabled on the downstream (DMZ) server, and adds/changes should be made only on the upstream (LAN) server.

Reduced Bandwidth for Remote Sites

If MBG is providing access for a remote office environment where the users often call one another, an MBG server can be provided on site and daisy-chained to the MBG server at the main office. This is not needed for MiNet to MiNet calls behind the same remote NAT because the MBG local streaming feature will handle that case. However, this deployment can be used to keep MiNet to SIP calls in the remote office. This configuration, illustrated in Figure 10, can save bandwidth on the link between the remote and main offices.

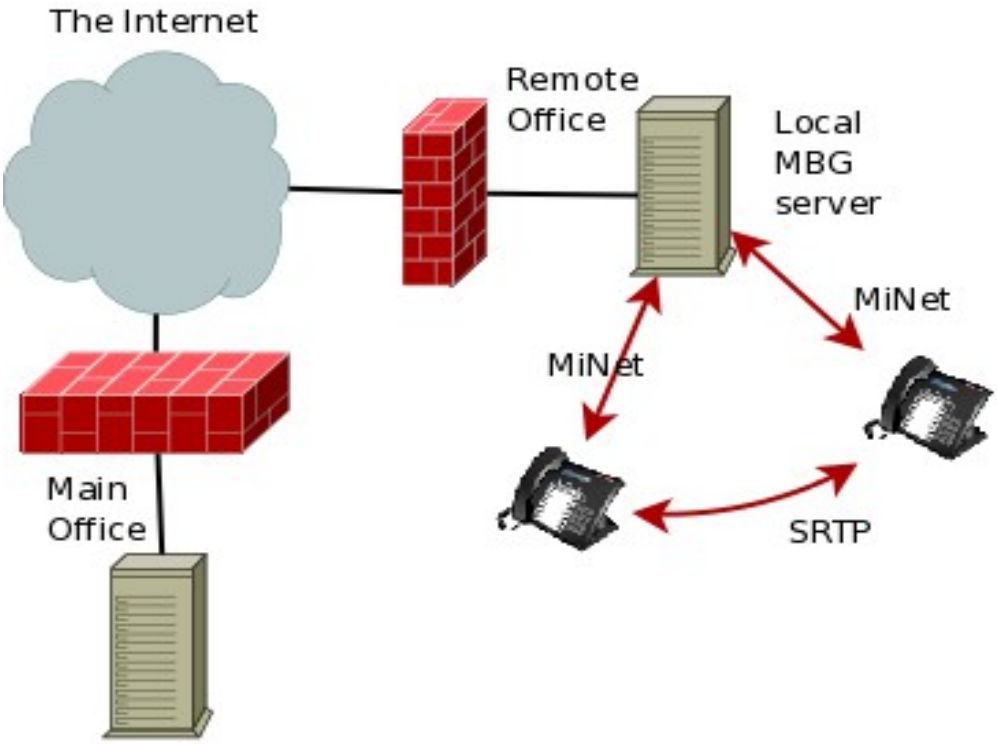


Figure 10: Daisy-chained MBGs to save bandwidth

The upstream server can be deployed in either a Gateway or a DMZ configuration.

Warning: Management of all remote office sets must be done on the upstream (main office) server only. When the downstream server is put into daisy-chain mode, it will automatically disable all MiNet and SIP connection restrictions, and pass all connection attempts up to the upstream server for authentication.

The remote office (downstream) MBG can also be configured for either a Gateway or DMZ deployment. Note that there is no restriction on the location of the remote office sets; they do not have to be on the LAN. It may be desirable to configure certain teleworker sets to connect to remote office MBGs (rather than the main office MBG) in order to cause direct streaming of those teleworkers' calls to sets in the remote office. This case requires Local streaming to be enabled on the upstream (main office) server.

It is even possible to deploy multiple downstream MBG servers at different remote offices. If upstream (main office) server has Local Streaming enabled, calls within each remote office remain local to that office: signaling

still flows back to the main office, but voice streams for calls between offices will only traverse the path between the two MBGs. This minimizes bandwidth use on the main office's connection.

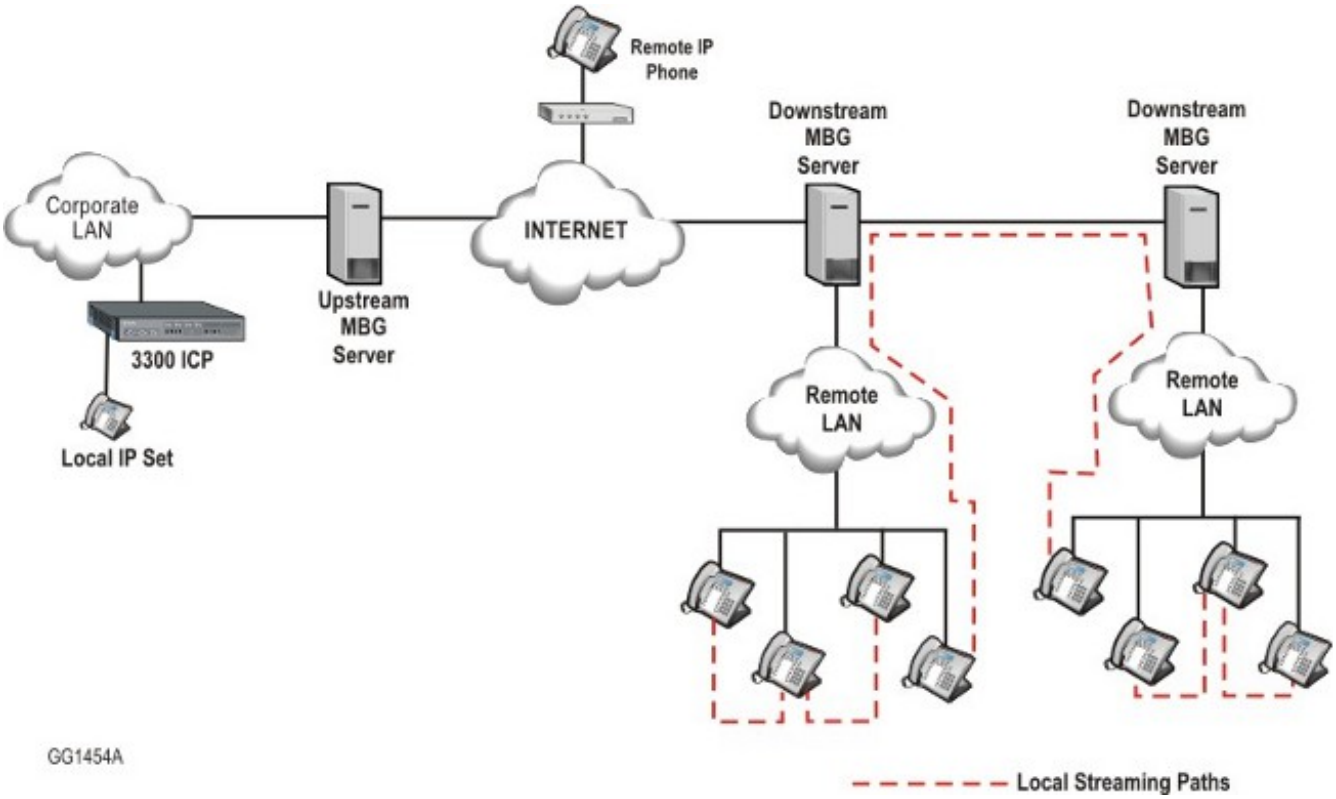


Figure 11: Multiple downstream MBGs

Caveat: All MBG servers in the daisy chain must be at the same release.

Refer to the *MBG Installation and Maintenance Guide* for a full description of setting up daisy-chaining.

2.8 MBG in MAS

There are two supported deployments of MBG in MAS: on the LAN and on the network edge (Gateway mode). Deployment in the DMZ is not supported.

MAS on the LAN

The safest way to deploy MBG is to leave MAS and its applications on the LAN, and deploy a second server running MBG (either standalone or single-app MAS) in the DMZ or in Gateway mode at the network edge. Remote access to the LAN MAS can be provided via Web Proxy on Internet-facing MBG. If centralized management is desired, the two MBG applications can be clustered. All changes made on the LAN server will be reflected on the edge MBG. Refer to the MAS documentation set for details on clustering MBG with MAS.

MAS on the Network Edge

Although Mitel recommends the dual server approach for maximum security, a single MAS server with all applications can be deployed in Gateway mode at the network edge. In this configuration, all administrative and end-user web interfaces and all services are directly reachable from the public network; Web Proxy is not required to reach them.

2.9 MBG in vUCC

The vUCC product combines MAS and MCD on one virtual machine. Refer to the vUCC Deployment Guide for a description of supported vUCC configurations.

Support for an additional MBG deployment configuration is introduced for vUCC environments only because of specific IT constraints imposed by some cloud providers. For vUCC deployments only, MBG in server-gateway behind an existing firewall is supported with the constraint that phones must not connect to the MBG from the LAN side of the firewall. That is, this configuration is only supported for phones connecting to the MBG WAN interface via the existing firewall WAN interface.

2.10 Partial Service Configurations

All MBG services are not available in all supported configurations. This section identifies for each MBG service configurations where the service is not supported at the time of writing. In some cases the service may be technically possible but not currently supported pending further testing or to reduce complexity.

MBG provides the following services:

- **Remote MiNet IP Phones**
  - Connecting to MBG in vUCC is not supported for LAN phones.
  - Connecting to MBG in MAS on the LAN is not supported for Internet phones.
- **Remote SIP IP Phones**
  - Connecting to MBG in vUCC is not supported for LAN phones.
  - Connecting to MBG in MAS on the LAN is not supported for Internet phones.
  - The SIP Teleworker service is not available with MBG for the following ICP type: 5000
- **SIP Trunking**
  - Connecting to a SIP trunk service provider from MBG in MAS on the LAN is not supported.
- **Call Recording**
  - Connecting to MBG in vUCC is not supported for LAN phones.
  - Recording calls with MBG in MAS on the network edge is not supported for LAN phones.
  - Recording calls with standalone MBG on the network edge is not supported for LAN phones.
  - Call recording is not available with MBG for the following ICP types: 5000, silhouette
- **Remote Proxy Services**
  - Remote Proxy Services are not available with MBG in MAS.
  - Remote Proxy Services are not available with MBG in vUCC.
  - Remote Proxy Services are not available with MBG for the following ICP types: 5000, silhouette.

3 Common Requirements

This section provides general guidance common to all types of deployments and all services. Please read it carefully.

3.1 Supported ICP Versions

At least one of the following compatible ICP products is required to use Mitel Border Gateway:

- Mitel Communications Director (MCD) release 4.0 or later. (Includes vMCD, MICD, 3300 platforms.)
- Broadview Networks *silhouette* release 4.0.0.3 or later. (Contact Broadview for the required MBG version.)
- Mitel 5000 CP. (SIP Trunking only for release 5, add MiNet Teleworker with release 6)

3.2 Administrative Access

MBG provides a web-based management GUI for normal administration, log access, etc. This service can be accessed with any of the following supported web browsers:

- Mozilla Firefox 3.0 or higher
- Microsoft Internet Explorer 6.0 or higher

Although not officially supported, the following browsers are tested occasionally and should also work:

- Google Chrome
- Apple Safari
- any browser using the Mozilla *Gecko* engine or the Apple *WebKit* engine

Note: the MBG GUI requires a browser that supports JavaScript. The built-in MSL text-mode browser does not support JavaScript and cannot be used to manage MBG.

Some troubleshooting or advanced configuration requires command-line access. SSH is the only supported mechanism to reach the MSL command line remotely. On Microsoft Windows, Mitel recommends the use of *PuTTY* (a small, free SSH client). *OpenSSH* is included with Apple Mac OS X (open Terminal and type “ssh”), and is included with or available for most flavors of Unix.

3.3 Firewalls (DMZ deployment)

MBG can be deployed into the DMZ of most third-party firewalls. However, a compatible firewall must have certain characteristics.

1. The firewall must provide at least three interfaces: external network, internal network, and DMZ.
2. The firewall must provide static 1:1 NAT between an externally-visible address and the DMZ address of the MBG server.
3. The public address used for MBG must be a static IP address visible from the external network (Internet). This should be a separate address from the external IP address of the firewall, although some firewalls that support port forwarding may allow sharing the address. It is vital that this address actually be static as any change of the address will cause remote sets to lose connectivity.
4. The firewall must preserve the TCP and UDP port numbers in packets exchanged between the MBG and the external network. In other words, only the address field may be changed.

For deployment in a DMZ, MSL must be installed in “server-only” mode with only a single NIC configured. This

NIC should be given an address on the DMZ network. The firewall will map between this address and the external address used for MBG.

Details of the protocols that must be configured in the firewall are provided in *Firewall Configuration*. Particular attention should be paid to the requirement that all UDP ports >= 1024 on the LAN be permitted to reach the public IP of the MBG server.

Warning: Failure to configure the firewall properly will result in audio problems (typically one-way audio).

Known Issues

Checkpoint “NG” Firewalls

Checkpoint “NG” firewalls (e.g. FireWall-1 NG) have a feature called “Smart Connection Re-use” that may interfere with older MiNet sets and some SIP sets that use a fixed source port for their outgoing connection. The feature should be disabled with older sets or if set connections to the MBG server cannot be maintained.

It is not a problem with newer sets that randomize the source port used for each new connection.

Port-Forwarding Firewalls

Use of MBG server with a port-forwarding firewall (where the external address of the firewall is shared between the Mitel Border Gateway and other applications) is supported by MBG version 3.0 and higher. The firewall device must have at least 3 interfaces (external, internal, DMZ). This allows for a single external IP address to be assigned to the firewall. It does not eliminate the need for a separate DMZ network.

This special configuration is identical to a normal DMZ deployment with the exception that the MBG’s publicly-visible IP address will be the same as the firewall’s publicly-visible address (that is, the single public IP address is shared).

Warning: Two-port firewall devices that simulate a DMZ through port forwarding are *not supported*, even if the device allows multiple external IP addresses.

SIP-Aware Firewalls

Many firewall devices today understand the SIP protocol and include some type of NAT traversal or rewriting of SIP packets. When MBG is used for connecting SIP clients (sets) and trunks, Mitel recommends turning off any SIP features of the main firewall. At best, it is redundant to have two devices performing the same job. In worse cases, they interfere with each other.

UDP Flood Protection

UDP flooding protection and VoIP applications utilizing RTP do not work well together. It is recommended that UDP flooding protection in firewalls in the voice path be disabled.

Firewall Configuration Common to all Services

In a DMZ deployment, it is recommended that the administrator configure their firewall in the following way, regardless of the MBG feature set in use:

- Allow return traffic from established TCP connections
- From the server to the Internet allow traffic with
  - protocol TCP, destination port 22 *(communications with Mitel AMC)*
  - protocol UDP, destination port 53 (and return traffic) *(DNS)*
- From anywhere to the server allow traffic with
  - protocol UDP, destination port range 20000 to the configured upper bound (31000 by default) *(RTP)*
- From the server to anywhere allow traffic with
  - protocol UDP, destination port >= 1024 *(RTP)*

Note: This list is not exhaustive. Refer to the sections on individual services for the required ports and protocols of each. A more comprehensive set of firewall rules is given in Appendix A: Firewall Configuration Reference.

4 Remote Phone Access

A major purpose of the MBG is to allow remote MiNet IP and/or SIP phones to connect to the office PBX over an insecure wide-area network such as the Internet, as if they were physically in the office. Most current (and many older) models of IP sets are supported by MBG. However, please refer to the *Remote IP Phones Configuration Guide* for guidance on specific models. Most SIP devices, including all Mitel-branded SIP devices, can also be configured to work with MBG.

This section provides general guidelines for the Teleworker service. Please refer to *Sizing Your Installation* to determine detailed requirements and performance limits.

4.1 Remote Site Requirements

Router

A set in a remote site (such as a home or branch office) is assumed to be part of a wired or wireless LAN behind a simple NAT router that provides access to the Internet, typically through a DSL or cable modem.

Mitel IP and SIP phones generally require a 10/100/1000 Mbps Ethernet connection, although some models can be configured for WiFi. (Refer to the device's documentation for configuration details.) All devices expect a TCP/IP network regardless of the link-layer technology.

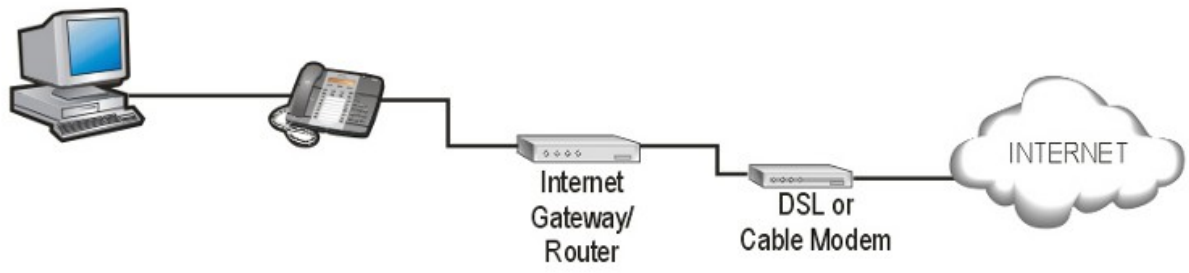


Figure 12: Example of a remote site

The remote site router must provide, at minimum:

- 10/100/1000 Mbps Ethernet with RJ45 connectors, for Mitel sets and connection to cable/DSL modem
- NAT from the internal network to the external network
- passthrough of UDP and TCP protocols, including TFTP

The router should provide DHCP service, offering at least an IP address and default gateway. However, devices can be programmed with static IP addresses and settings in the absence of DHCP.

The router may need to support PPPoE/PPPoA when used with a DSL modem, and must be configured with the user name and password provided by the ISP.

The router may need to support Authenticated DHCP (client) when used with a cable modem, and must be configured with the user name and password provided by the ISP.

If WiFi sets are to be used, the router or a separate WiFi access point must also provide 802.11 b/g/n.

The router must control the Internet connection in order for multiple devices to share the connection. When using desktop phones, the use of USB PPPoE/PPPoA modems, USB 3G/4G modems, etc are not supported as they do not provide a port to plug in the phone. However, such devices can be used with softphones running on the PC if no other devices need to share the internet connection of the PC. A similar caveat applies to any service that requires software to be loaded on the PC, such as AOL Broadband. It cannot be used with a desktop device, but can possibly be used with a softphone application such as Mitel Unified Communicator Advanced.

Note: the remote site may have a dynamic IP address. However, if the address changes during a call, the call will drop and all devices at the site must re-register with MBG to restore service.

VPN Connectivity

Connecting a PC to the second Ethernet port on the back of a Mitel IP phone does not provide the PC with a VPN connection to the office network. That connection must still be made by use of the organization's supported VPN client software. This ensures that security of the corporate network is maintained when using Mitel Border Gateway.

A gateway-to-gateway VPN can be constructed between branch offices (or homes) and the main office, if desired, such that all the PCs in the remote office have full access to the corporate LAN. However, Mitel advises that only non-voice traffic be routed across the VPN; voice traffic between sets and the MBG should traverse the Internet whenever possible. Routing real-time voice protocols across a VPN can result in degraded service.

Mitel Standard Linux, upon which MBG runs, does provide a PPTP VPN service. If desired, the MBG server can be used as a VPN concentrator for access to the corporate network. However, a VPN is not required to use the features of MBG itself. For more details, please see the *Mitel Standard Linux Installation & Administration Guide (*available from http://edocs.mitel.com/).

Using an Existing VPN

Using the Mitel Border Gateway does not affect any existing VPN client software (e.g. IPSEC road warrior connection) installed on the remote PC. The PC should be connected to either the second Ethernet port of the IP phone or directly to the router and the existing software should be used as before.

Note: VPN (e.g.IPSEC) pass-through must be supported by the router at the remote site.

Corporate Firewall & Network Configuration for VPN Access

The corporate office firewall may need to be reconfigured to allow other traffic from the MSL server to the internal network if the MSL server is used as a VPN server. The ports and protocols required will depend on the applications used by the client PCs and this configuration is outside the scope of this document.

More information on firewall configuration can be found in 3.3 Firewalls (DMZ deployment) and Appendix A: Firewall Configuration Reference.

Bandwidth Requirements for the Remote Site

This section analyzes bandwidth requirements of the remote site using the Mitel Border Gateway. Typically, there will be other requirements for Internet access, and these requirements (such as e-mail, web browsing, e-

commerce) must be provisioned as well. Failure to provide sufficient bandwidth for all Internet activities may compromise the quality of service provided by the Mitel Border Gateway.

The table below shows examples of bandwidth required for various types of remote media streams.

Voice	If compression (G.729a) enabled: **24** Kbps (bi-directional) If compression not enabled (G.711): **80** Kbps (bi-directional)
MCA Collaboration	**192** Kbps (bi-directional)
UCA Video	**256** Kbps – **1600** Kbps (bi-directional)
UC360 Video	**512** Kbps – **1500** Kbps (bi-directional)

Table 1: Bandwidth requirements of a single remote teleworker device

This table does not consider bandwidth requirements for PCs or other devices, which must be provisioned in addition to the IP Phone. If there is insufficient bandwidth, symptoms experienced by the IP phone user may include degraded voice quality, slow response, service interruption or loss of service. It also does not consider bandwidth requirements for additional applications. Please see the section *Additional Application Requirements* for more information.

Note: A video call requires 10 to 20 times more bandwidth than a compressed audio call even when configured with the lowest bandwidth settings.

A remote UC360 connecting to MBG over the Internet should be configured to disable the H.264 High Profile codec and to disable the Dynamic Bandwidth Allocation option. A video conference should not be initiated from a UC360 on the Internet because it would serve as a bridge and dramatically increase bandwidth requirements for the call.

Video calls between UCA 6.0 and UC360 2.0 are supported through MBG but they do not negotiate bandwidth at the time of writing. For example, a UCA client on the Internet will receive video at the rate configured on a UC360 on the LAN even if the UCA is configured to use low bandwidth. This will be rectified in a future release of UCA and/or UC 360.

MCA voice and video conferencing between MCA clients via the MCA server is also supported through MBG. The bandwidth usage per video stream is configurable on the MCA client. An additional consideration is that an MCA client can receive multiple video streams, one for each video participant in the conference. That number can be reduced at the MCA client by minimizing or closing video windows.

For details and current values, please see the engineering guidelines for the devices/applications referenced as examples here *(*available from http://edocs.mitel.com/).

Bandwidth Usage and ISP Quotas

Many Internet Service Providers set quotas on the amount of IP bandwidth per month. As an aid in predicting whether a specific quota will be exceeded, this section provides the necessary data and a sample calculation.

Assumptions:

- Signaling channel requires 1 KByte per minute (average), based on 6 calls per hour, business usage, 15 minutes per hour
- Options keepalive and Gap registration enabled for SIP, at 20s and 300s respectively

	Bandwidth Required	Hourly Usage (100%)	Monthly Usage (100%)
Signaling (MiNet)	1 KB/minute	60 KB	43.2 MB
Signaling (SIP)	1.75 KB/minute	105 KB	75.6 MB
G.711 voice stream (IP), 20ms	80 kbps	36 MB	25.92 GB
G.729a voice stream (IP), 20ms	24 kbps	10.8 MB	7.78 GB

Table 2: Bandwidth usage vs time for an IP or SIP phone

Note: 20ms is the default RTP frame size, but the value is configurable in the Mitel Border Gateway administration panel.

The data in the above table can be used to:

1. estimate the available call time given a quota
2. estimate the monthly bandwidth requirement for a given call volume

Example 1: Estimating Available Call Time

Given an ISP quota of 2 GB/month and continuous use:

Call hours of G.729a = (2000 MB - 43.2 MB) / 10.8 MB per hour = 181 hours

Call hours of G.711 = (2000 MB - 43.2 MB) / 36 MB per hour = 54 hours

Given the same 2 GB/month quota, and usage of 15 min/hr, 12 hours per day, 7 days per week:

Call hours of G.729a = (1448 hours or more than 1 month)

Call hours of G.711 = (432 hours or roughly 18 days)

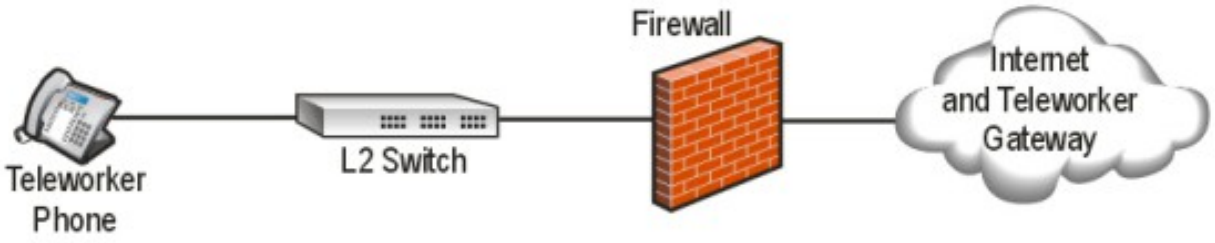
Example 2: Estimating Monthly Bandwidth Requirements

Given a user that averages 4 hours of phone calls per day, for 22 workdays in a month:

Bandwidth Usage for G.729a = 43.2 MB + (10.8 MB x 4 hr per day x 22 days) = 994 MB

Bandwidth Usage for G.711 = 43.2 MB + (36 MB x 4 hr per day x 22 days) = 3200 MB or 3.2 GB

Configuring the Remote Site Firewall



If the remote office has a firewall, it must be configured to allow the IP or SIP phone to connect through it to the Mitel Border Gateway. The simplest approach is to permit all connections to or from the MBG's IP address. A second very simple approach is to permit all outgoing connections and any responses to them. By default, most

small office and home NAT routers allow outgoing connections and responses to those outgoing connections.

Sites with more restrictive security policies may wish to use the following rules:

- Allow a bi-directional TCP connection to destination ports 6801 and 6802 on Mitel Border Gateway IP address
- Allow bi-directional TCP connections to destination ports 3998 and 6880 on the Mitel Border Gateway IP address (for 5235, 5330, 5340 and Navigator set features)
- Allow incoming UDP from source ports 20000 to 31000 on Mitel Border Gateway IP address
- Allow outgoing UDP to destination ports 20000 to 31000 on Mitel Border Gateway IP address
- Allow bi-directional TCP connections to destination ports 36005, 36006, 36007, 36008 and 37000 on the Mitel Border Gateway IP address, if using UCA.
- Allow incoming and outgoing UDP to port 5060 on the Mitel Border Gateway IP address, if SIP support is desired

4.2 TFTP Behavior

Mitel IP phones require a TFTP server that holds their set firmware and HTML applications. For remote phones, this TFTP service is provided by MBG.

Previous versions of MBG bundled a version of the HTML Applications and served them directly. This caused some trouble with keeping versions in sync, especially with multiple ICPs. Since release 7.0, MBG does a proxy request to the appropriate ICP instead.

When an IP phone connects to its ICP, the ICP (MCD) may issue a File Download directive over the SAC protocol connection. MBG intercepts these directives and downloads the file on behalf of the remote set. It then sends a modified directive to the set instructing it to download the cached file from MBG. This ensures that the set receives the same file that it would if it were directly connected to MCD. MBG will check periodically for updated HTML application files at the ICP. The frequency of checks depends on the feature set supported by the ICP. It could be as often as 10 minutes, and as infrequent as 24 hours.

Note: MBG's file downloader does not know about any ICPs until sets connect to MBG and thus get connected to an ICP. This step happens after a set has already retrieved its firmware load via TFTP. Due to that, set firmware loads are still bundled with MBG and are not fetched from the ICPs.

4.3 Firewall Configuration for Remote MiNet Devices

When MBG is deployed in the DMZ, the corporate firewall protecting the DMZ requires the following rules (in addition to the common rules found in *Firewalls (DMZ deployment)):*

From the Internet to the MBG server:

- allow protocol TCP, destination ports 6801, 6802[2], 3998 and 6881
- allow protocol UDP, destination port 20001 (and return traffic)

From the MBG server to the LAN (or just ICPs):

- allow protocol TCP, destination ports 6800, 6801, 6802, 3998, 3999 and 6880
- allow protocol UDP, destination port 20001 (and return traffic)

Note: This is a minimal configuration. Refer to *Appendix A: Firewall Configuration Reference* for the full set of rules and optional settings.

2 Port 6802 is not required for Enhanced Security mode

4.4 Configuring MBG for Remote SIP Devices

Remote SIP Device Limitations

MBG cannot yet load-balance SIP devices. In general, resiliency for a SIP device can be achieved through external DNS by configuring multiple “A” records for the FQDN of the MBG, or by configuring SRV records. Refer to the documentation of the remote SIP devices for guidance on configuring resiliency.

Tuning Global Parameters

The default values for all parameters assume a Teleworking installation, with SIP devices being used over the Internet. In a LAN context, these parameters will work correctly but may be slightly aggressive.

By default, MBG sends a SIP “Options” request to every connected device at an interval of 20s (“Options keepalives”). The responses from these requests reset the idle timer for each connection. Each connection has a 300s (5 minutes) idle timeout, so the most important thing to remember is that the MBG server must see valid SIP traffic from each device within the 300s interval. A device that times out due to inactivity is disconnected and becomes out of service.

On a “quiet” network it is sufficient to disable gapped registration and raise the options interval to its maximum value (180s at this time). If all remote SIP devices send their own keepalives or re-register at an interval less than 300s, MBG's Options Keepalives can be turned off.

DNS Support

While SIP clients can address MBG by its IP address, Mitel recommends the use of a fully-qualified domain name (FQDN) in the public Domain Name System (DNS) that resolves to the public IP of the MBG server.

Advantages:

- The IP address of the MBG server can be changed, and the clients will not need to be reconfigured.
- DNS can provide a certain level of resiliency in case an MBG server experiences any kind of service outage. Simply configure the FQDN to resolve to multiple MBG servers. Please note that MBG cannot control how a SIP device behaves when it receives multiple IP addresses in a DNS response.

Note: A remote SIP message will be recognized as being addressed to MBG if the IP in the URI is one that MBG owns, or the FQDN in the URI either resolves to an IP that MBG owns, or is one of the configured “Allowed URIs” in the “SIP options” section of the Configuration tab.

Warning: A SIP server requires functional DNS even if all devices are configured to use IP addresses instead of FQDNs. MBG is no exception. Failure to provide MBG with a working DNS resolver or preventing MBG from reaching the Internet DNS root servers can cause delays or failures in call setup.

4.5 Firewall Configuration for Remote SIP Devices

When MBG is deployed in the DMZ, the corporate firewall protecting the DMZ requires the following rules (in addition to the common rules found in *Firewalls (DMZ deployment)):*

From the Internet to the MBG server:

- allow protocol UDP, destination port 5060 (and return traffic)

From the MBG server to the LAN (or just ICPs):

- allow protocol UDP, destination port 5060 (and return traffic)

Note: This is a minimal configuration. Refer to *Appendix A: Firewall Configuration Reference* for the full set of rules and optional settings.

5 SIP Trunking

5.1 Overview

A “SIP trunk” in the context of MBG is simply a pair of endpoints, defined by their IP addresses and signaling ports. One of the endpoints is usually your ICP (MCD (3300 ICP) or 5000 CP), and the other is your SIP provider’s firewall or SBC.

A trunk can have any number of “channels,” each of which corresponds to an active media stream. A channel license is required for each active channel, so you will need enough channel licenses to cover the maximum number of active calls. As an analogy, an ISDN PRI link contains 23 B channels for audio and one D channel for signaling, and can carry a maximum of 23 simultaneous calls. This would be equivalent to a SIP trunk with 23 channel licenses.

Note: On the MCD (3300 ICP), the MBG is configured as an outbound proxy in the Network Element form.

Warning: In the 5.X releases, the SIP trunk connector listened on UDP port 5064 by default. As of MBG 6.0 the SIP connector can handle device endpoints and sip trunks, so UDP port 5060 is used for both devices and SIP trunks. The Legacy Connector can no longer be re enabled as of MBG 8.0. If UDP port 5064 is in use then you will need to contact your SIP Trunk provider to have their equipment changed to use MBG's UDP port 5060 before upgrading MBG to 8.0.

Warning: A SIP server requires functional DNS even if all devices are configured to use IP addresses instead of FQDNs. MBG is no exception. Failure to provide MBG with a working DNS resolver or preventing MBG from reaching the Internet DNS root servers can cause delays or failures in call setup.

5.2 Bandwidth Requirements

Please see the section *Sizing Your Installation* on page 40.

5.3 Resilient Trunk Configuration

This section describes a sample resilient SIP trunk configuration using two ICPs and two MBGs.

First, configure resiliency between the ICPs.

On ICP “A”:

- Create a Network Element Assignment for MBG “A” (as type Outbound Proxy) and another for the SIP provider’s SBC (as type Other). Create a SIP Peer Profile for the SBC using MBG “A” as the Outbound Proxy.
- Add a Network Element Assignment for MBG “B” (as type Outbound Proxy) and create another SIP Peer Profile for the SBC using MBG “B” as the Outbound Proxy.
- Program a Route List in ARS with SIP peer “A” and SIP peer “B”. Then program ARS Digits Dialed such that outgoing calls use the new route list.

Repeat the above configuration on ICP “B”, except reverse the order of trunks in the route list so that “B” comes before “A”.

Configure MBG clustering. On the master MBG, go to the “ICPs” tab and add both ICP “A” and ICP “B”. On the “SIP Trunking” tab, configure a trunk profile for the remote SBC. Add a single routing rule of “*” with ICP “A” and ICP “B” as the targets of the rule. This configuration will propagate to the secondary MBG.

Incoming calls from the SBC will arrive at either MBG A or MBG B. From there, the MBG will route them to ICP A if it is up, or to ICP B if ICP A is down. Outgoing calls from either ICP can be routed through either MBG.

5.4 DNS Support

While the ICP can address MBG by its IP address, Mitel recommends the use of a fully-qualified domain name (FQDN) in the public Domain Name System (DNS) that resolves to the public IP of the MBG server.

Advantage:

- The IP address of the MBG server can be changed, and the ICPs will not need to be reconfigured.

Note: An ICP SIP message will be recognized as being addressed to MBG if the IP in the URI is one that MBG owns, or the FQDN in the URI either resolves to an IP that MBG owns, or is one of the configured “Allowed URIs” in the “SIP options” section of the Configuration tab. Typically, the hostnames youadd to the “Allowed URIs” list will be for the SIP service provider's session border controller or service domain.

Warning: A SIP server requires functional DNS even if ICPs are configured to use IP addresses instead of FQDNs. MBG is no exception. Failure to provide MBG with a working DNS resolver or preventing MBG from reaching the Internet DNS root servers can cause delays or failures in call setup.

5.5 Firewall Configuration for SIP Trunking

When MBG is deployed in the DMZ, the corporate firewall protecting the DMZ requires the following rules (in addition to the common rules found in *Firewalls (DMZ deployment)):*

Note: Please remember to turn off any UDP flooding protection and any SIP features of the DMZ firewall.

From the Internet to the MBG server:

- allow protocol UDP, destination port 5060 (and return traffic)

From the MBG server to the LAN (or just ICPs):

- allow protocol UDP, destination port 5060 (and return traffic)

Note: This is a minimal configuration. Refer to *Appendix A: Firewall Configuration Reference* for the full set of rules and optional settings.

6 Call Recording

MBG includes the ability to act as a secure man-in-the-middle for SRTP voice streams, enabling a third-party call recording solution to tap calls by using MBG's SRC interface.

Please see the section on *Sizing Your Installation* to determine performance limits and resource requirements.

6.1 Call recording vs. Local streaming

Mitel Border Gateway supports both Local Streaming and Call Recording, both of which can be enabled or disabled for individual users. These options are not compatible.

Local Streaming is a generally desirable feature that reduces bandwidth needed for voice/video calls by allowing the RTP stream(s) to bypass the MBG when two devices are able to communicate directly. However, this means such calls cannot be recorded. *If both Local Streaming and Call Recording are enabled on a device, Call Recording wins*. All streams to and from that device will go through MBG so they can be recorded.

6.2 Indirect Call Recording

Indirect Call Recording (ICR), introduced in MBG 7.1, is a feature supported by Mitel's 53XX series IP sets and MCD software release 5.0 SP1 and up. It also has only limited support from CRE vendors.

With ICR in place, SRC can support recording of any supported sets that are connected to any supported MCD without having to reconfigure the sets to connect through SRC, as is the case with "direct" call recording. SRC can be configured with a mix of both ICR and "direct" call recording. This would be required if non-supported sets or MCDs are deployed.

Using ICR allows for some cost reductions and more network flexibility in certain call recording deployments. It is especially applicable for network deployments where centralized call recording is desired in a network situation where remote, WAN-connected sets are connected to remote office MCD's.

When MBG is deployed in the DMZ, the corporate firewall protecting the DMZ requires the following rules (in addition to the common rules found in *Firewalls (DMZ deployment))* to support Indirect Call Recording*:*

From the MBG server to the ICPs:

- allow protocol TCP, destination port 6815 (and return traffic)

7 Additional Application Requirements

MBG allows the use of several supported applications from remote sites, just as it allows use of IP phones. When MBG is deployed in the DMZ of a third-party firewall, that firewall must be configured to allow connections from these applications.

This section, plus the common rules in *Firewalls (DMZ deployment)* on page 15, gives a minimum configuration for each supported application. Refer to *Appendix A: Firewall Configuration Reference* for the full set of firewall rules.

7.1 Unified Communicator Advanced (UCA) v4.0+

Warning: MBG 7.0 required a port-forwarding rule for port 36008 that directed traffic to the UCA server. After upgrading to MBG 7.1 or higher, this rule must be removed from the MSL Port Forwarding panel.

The following additional rules are required, excluding the UCA softphones:

From the Internet to the MBG server:

- allow protocol TCP, destination ports 5269, 36005 – 36008 (inclusive)

From the MBG server to the LAN:

- allow protocol TCP, destination ports 80, 443, 5060, 5269, 36008

Note: When UCA server is behind MBG, remote UCA clients require access via Web Proxy for UCA 5.1 and above. See 7.3Web Proxy for additional firewall rules.

UCA clients also include MiNet and SIP softphones. For additional firewall rules covering the UCA softphones see 4.3 Firewall Configuration for Remote MiNet Devices and 4.4 Configuring MBG for Remote SIP Devices.

MBG 8.0 includes two additional connectors to help with specific kinds of UCA SIP softphone connectivity issues that may be experienced in some deployments due to improper handling of SIP UDP by some NAT firewalls. These MBG connectors allow the configuration on selected UCA SIP softphones to be changed from SIP UDP signaling to use SIP TCP or SIP TLS signaling (TLS preferred). When the selected UCA SIP softphone connects to MBG on TCP or TLS from the Internet, the MBG bridges it internally to the SIP UDP connector used by default for the unmodified UCA SIP softphones.

The following additional rules are required for UCA SIP softphone signaling over TCP or TLS:

From the Internet to the MBG server:

- allow protocol TCP, destination ports 5060, 5061

7.2 Mitel Contact Center

The following additional rules are required:

From the Internet to the MBG server:

- allow protocol TCP, destination ports 35001 – 35008 (inclusive), 36000 – 36004 (inclusive)

From the MBG server to the LAN:

- allow protocol TCP, destination ports 80, 443, 1443, 5024 – 5026 (inclusive), 5030, 7001, 7003, 8083, 8084, 8188, 42440

7.3 Web Proxy

The following additional rules are required, at minimum:

From the Internet to the MBG server:

- allow protocol TCP, destination port 443

From the MBG server to the LAN:

- allow protocol TCP, destination port 443

Special consideration for MCA through Web Proxy

In addition to https traffic, MCA requires passthrough of its ConnectionPoint connection. It will arrive at the firewall on TCP port 443, on a dedicated IP address for MCA (see the MAS documentation for full details), and the firewall must forward the traffic to the Web Proxy server (MBG) at whatever listen port is configured in Web Proxy.

From there, the traffic will be forwarded to the MCA server on the LAN on TCP port 4443. The required rules are:

From the Internet to the Firewall:

- allow protocol TCP, destination port 443 on the MCA IP address

From the Firewall to the Web Proxy (MBG):

- allow protocol TCP, destination port A, where A is the listen port for MCA configured by the Web Proxy administrator

From the Web Proxy (MBG) to the MCA server on the LAN:

- allow protocol TCP, destination port 4443

7.4 Remote Management Service

MBG Remote Proxy Services includes Web Proxy for end users and Remote Management Service for system administrators. The Remote Management Service introduced a new capability in MBG 8.0 to support remote upgrade, backup and restore of MCDs on the LAN. This feature requires enabling an FTP server on the MBG. Remote FTP clients on the external network upload MCD software to the FTP server on MBG. An MCD FTP client on the internal network downloads MCD software from the FTP server on MBG. An MCD FTP client on the internal network uploads MCD backup files to the FTP server on MBG.

Note: Remote FTP clients must use passive FTP. Active FTP will not work through remote NAT firewalls.

The following additional rules are required, at minimum:

From the Internet to the MBG server:

- allow protocol TCP, source ports >1023, destination port 21, destination ports >1023

From the MCD on the LAN to the MBG server:

- allow protocol TCP, source ports >1023, destination port 21, destination ports >1023

8 Additional Security Considerations

Due to the broad range of application types that can be deployed on the Mitel Standard Linux operating system (formerly Managed Application Server), Mitel suggests that you read the Security section of the Mitel Standard Linux Installation and Administration Guide before installing this application on the same server with other applications,

8.1 SIP Security

While the majority of traffic in MBG is encrypted, the SIP implementation is UDP-based, and unencrypted at this time. Additionally the RTP streams for SIP voice & video calls are also plain RTP, and thus unencrypted. As our SIP implementation cannot make use of SRTP at this time, calls between SIP and MiNet sets are also “in the clear”.

This will be rectified in a future release.

9 Traffic Shaping

9.1 Overview

For small businesses with a simple setup to the Internet, sharing that upstream link between voice and data can be problematic. Users in the middle of calls to the PSTN via SIP trunks, for example, will find the voice quality of their calls greatly reduced if a member of the office were to suddenly start a large download from the Internet. To mitigate these issues, MBG has the capability to prioritize the IP traffic that it is handling. This technique is commonly known as *traffic shaping*.

To shape traffic, MBG must be in a position to handle all traffic to the organization's upstream link; specifically, it must be in gateway mode with a minimum of two network interfaces. In this mode, it can act as the organization's firewall. More commonly, however, the organization already has a firewall product of some kind, and would like to deploy MBG and use traffic shaping with a minimum of disruption. This "transparent" deployment is possible on servers with three network interfaces.

Using MSL 9.2+ the third interface can be put into *bridged mode.* The bridged interface can then be connected to the WAN interface on the existing firewall. This configuration transparently places MBG between the existing firewall and the WAN, and allows MBG to prioritize the organization's traffic, without requiring changes to the existing firewall.

9.2 Technical Details

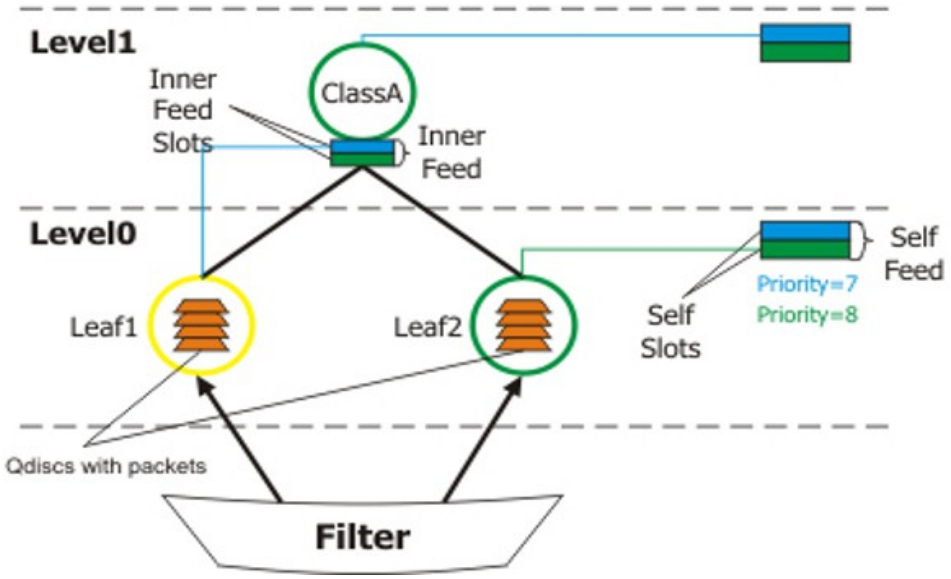
Figure 13 below illustrates the queuing discipline that MBG uses for traffic shaping. The hierarchical nature of the algorithm allows lower priority queues to use tokens available in higher priority queues, which means that when little VoIP traffic is available, lower priority data will not be unnecessarily constrained. Thus, the customer can make full use of their available bandwidth to the Internet.

The categorization of high priority vs. low priority traffic is performed based on two criteria:

1. **Source IP Address** If the source IP address of the traffic belongs to any of the network interfaces on the MBG server, then it matches the first criteria. In other words, MBG must originate the traffic.
2. **DSCP value** The second criteria of high priority traffic is a DSCP value of 46 decimal, 0x2E hex (Expedited Forwarding). This value must be set on packets that are considered high priority. MBG will set the value for its own VoIP-related traffic.

If both of these criteria are satisfied, then the traffic ends up in the high priority queue. Otherwise, it is considered low priority and will only be permitted through the HTB queue if the high priority queue has unused tokens.

This does mean that excessive high priority traffic can starve low priority data traffic. However, 10% of available bandwidth is reserved for low priority traffic (if it is present), so it should not starve completely. This reservation does not waste bandwidth: it can be "borrowed" by the high priority queue if no low priority traffic is present.



(Image credit: http://www.mikrotik.com/testdocs/ros/2.9/root/queue.php)

Figure 13: The Hierarchical Token Bucket Queue

10 Clustering

10.1 Overview

Clustering in this context refers to the ability of multiple MBG servers to communicate with one another via TCP, sharing data and providing the capability to manage multiple nodes thus joined as if they were a single unit.

Clustering also provides load balancing for supported MiNet devices, making the job of distributing devices across servers to share workload simple and effective. Set resiliency is also used within clustering, so that supported MiNet sets which can persistently store up to four IP addresses will have their resiliency list populated based on the cluster members.

Clustering relies on a mesh of TCP connections between the nodes in the cluster. TCP port 6809 must be reachable between all nodes for cluster comms to be established. SSL/TLS is used to encrypt communications, so it is safe to use over the Internet.

Administrative access to each server in the cluster is required to establish a trust relationship between the nodes. The trust model is based on the IP addresses used to establish cluster comms. Each node is configured via the clustering tab to trust a connection coming in from a particular IP address. These addresses are shared across the cluster, so they must be reachable by all nodes involved, and any use of NAT will break the trust model. A summary of the steps to create a three-node cluster are shown below. Refer to the *Mitel Border Gateway Blade Installation and Maintenance Guide* for full instructions on creating a cluster.

- Create the cluster from the master node, entering the IP address of the first slave node.
- Join the cluster from the first slave node, entering the IP address of the master node.
- Assuming no networking issues, the clustering tab will show established connections, and the slave node will show a backlog of events from the master (or it will finish too quickly to be seen).
- Add a node on the master, entering the IP address of the second slave node
- At this time, the first slave will receive the same data regarding the second slave via cluster comms.
- Join the cluster on the second slave, entering the IP address of the master node.
- Assuming no networking issues, the clustering tab on all nodes should show the peer nodes for that node.
- The three node cluster is now established.

Once cluster communications are established, the master node will “push” data to the slaves until they are in sync with the master. Conflicting data is overwritten. Data that the master node does not have a copy of is not modified, and is not pushed to the master. Merging data is accomplished by taking ownership from each slave node (i.e. making that node the master) in turn, causing the new master to push its data to all other nodes, until all data is in sync across the cluster. Unwanted records can then be deleted from the master node.

10.2 Cluster Zones

A *cluster zone* is a non-overlapping subset of nodes within an existing cluster. All nodes start out in the “Default” zone. The “Default” zone can be renamed but it cannot be deleted. It is easily identified because it appears first in the zone list, and has no “delete” link. Nodes can be left in the default zone if additional zoning is not required.

Additional zones can be created, and nodes can be moved to any zone. Zones can be created based on geographic location, the intended purpose for the nodes, or whatever reason the admin chooses. The purpose of zones is to provide *device affinity*.

By default all MiNet sets will be associated with the default zone. By editing the set, the set may have its affinity changed to a different zone. The implications of this are as follows:

- A set's load-balancing list of nodes will always favor nodes in its zone
- The last entry in the load-balancing list will be a node from the default zone

This feature was introduced to support geographically dispersed clusters. For example, if there are three servers in North America and three in Asia, it makes little sense for Asian sets to be load balanced to North America unless all of the Asian servers are unreachable. Using cluster zones, a "North America" zone and an "Asia" zone could be created, and sets in Asia could be placed into the Asian zone. The sets in each region would then prefer the nodes in their region, reducing network latency and bandwidth use.

Similarly, zones can be created to segregate devices by function, such as keeping trials users on a separate node from regular users, or to split users by organizational group.

10.3 Node Weighting

Not all servers are created equal. If the hardware in the cluster is all equivalent, it is safe to leave the weight of each node in the cluster at its default value of 100. This ensures evenly-distributed load balancing.

To inform the cluster that a given node should handle more than an equal share of the load, increase its weight. If the server should handle less, lower the weight. For instance, assume there is a cluster of three nodes with weights of 50, 50, and 100. The two smaller servers (lower weights) will each handle roughly one quarter of the total load, while the third server handles the remaining half of the load.

Weights are not percentages[3]; they are simply a ratio of relative server power. Weights of 100,100,100 are equivalent to weights of 1,1,1. However, if the sum of all weights is 100 (or close to it), they can be treated as percentages of the total load and the system will behave as expected.

A weight of zero prevents any devices from connecting and will cause MBG to move all connected devices to other nodes.

Expressed mathematically, the above is simply:

sets_on_a_node = total_sets x (node_weight / sum(node_weights))

Note: the distribution of devices will not be mathematically perfect. Some hysteresis is built in to the load-balancing algorithm to prevent devices from being redirected too often in a vain attempt to perfectly balance the cluster.

Note that **weighting applies to *zones*, not to *clusters*.** The "total load" is the load from devices configured with the same zone as the node. (In a cluster with only the Default zone, this distinction can be ignored.)

As an example, consider a cluster with five nodes and two zones. Two servers are in the "North America" zone and two servers are in the "Asia Pacific" zone. The remaining server is left in the Default zone.

The two North America servers are identical and have weights of 10. Each one will handle roughly one half of the total load of devices configured for the North America zone. One of the Asia Pacific servers is new and has more capacity; it has a weight of 20 and the other server has a weight of 10. The newer server will handle twice as much load (roughly two thirds) as the other server (one third). The fifth server handles 100% of the load in the Default zone, regardless of its weight.

Warning: not all devices can be load-balanced. See *Additional Considerations* for details.

3 Note that using "total_sets = 100" in the formula below gives the percentage of total load handled by one node.

10.4 Additional Considerations

While heterogeneous server capabilities are supported in a cluster thanks to the weighting mechanism, this weighting only affects the number of connected devices on each server. The cluster communications adds additional load on each server, so adding a node to the cluster does not, necessarily, linearly increase the capabilities of the cluster.

Furthermore, if the master node is used as the initial point of contact for all devices, then it should not be a “weak” server. There are many supported devices that do not support redirection, so the server they are programmed to contact will be the only server that they connect to. Setting a low weight on the main node will not change this. **All SIP devices, MiNet softphones, and 5550 IP Console fall into this “non-redirectable” category. Such devices must be balanced manually by programming the devices to contact specific nodes.** Setting a low weight, or a weight of zero, on nodes that handle non-redirectable devices can help with manual load balancing.

10.5 Firewall Configuration for Clustering

When MBG is deployed in the DMZ, the corporate firewall protecting the DMZ requires the following rules (in addition to the common rules found in *Firewalls (DMZ deployment)):*

From each MBG server to all other MBG servers in the cluster:

- allow protocol TCP, destination port 6809

Note: This is a minimal configuration. Refer to *Appendix A: Firewall Configuration Reference* for the full set of rules and optional settings.

11 Advanced Options

11.1 Resiliency

Supported MiNet sets have a resiliency list of up to four IP addresses. If a set loses its connection and cannot reestablish, it will try the next IP address on its list until it has exhausted all IP addresses on its resiliency list. For MiNet sets supporting persistent resiliency lists, this resiliency list is “remembered” through a power cycle.

The resiliency list can be manually configured with arbitrary IP addresses. Ideally they correspond to multiple MBG servers, but that is up to the administrator.

In a clustered environment, Mitel recommends populating the resiliency list with nodes in the cluster. If the cluster is spread across a subnet boundary, include nodes from each subnet to prevent a single point of failure.

Note: The resiliency assignments do not in any way bind a given device to a specific node. Devices that do not support redirection (a subset of MiNet devices, plus any SIP devices) will stay with the server to which they initially connected. Clustering load balancing does consider devices that cannot be redirected.

11.2 IP Translations

Multiple servers deployed on the same DMZ need to each be addressable by individual public IPs so Teleworker clients can reach them. The IP addresses configured on their interfaces should be DMZ addresses, most likely from the RFC 1918 range to prevent routing to or from the DMZ without specific rules in the firewall and on the LAN. This presents a problem for MBG servers that need to stream to one another.

Consider an example of two servers, server A and server B, both installed in a DMZ configuration on the same DMZ.

	Public IP	DMZ IP
MBG A	66.46.21.11	192.168.0.5
MBG B	66.46.21.12	192.168.0.6

Set 1 connected to MBG-A calls set 2 connected to MBG-B. MBG-B intercepts the signaling and MBG-A sees a request to stream from set 1 to the public IP of MBG-B. If MBG-A streams to MBG-B via its public IP, there is a very strong possibility that the firewall will not permit the SRTP traffic to route back to the DMZ that it originated from, resulting in audio problems. Furthermore, it is a waste of bandwidth on the public side of the firewall to stream traffic out to it that is destined for a server on the same network once the firewall’s NAT rules take effect.

The solution is simple. Both problems are solved by streaming directly from MBG-A's to MBG-B using their DMZ addresses. Unfortunately MBG-A is not aware of the existence of MBG-B. This is the purpose of the IP Translations feature.

In the MBG management GUI, choose Configuration and then IP Translations. In this example, the administrator would enter the following rule on MBG-A:

Destination address: 66.46.21.12
Translation address: 192.168.0.6

Now when MBG-A encounters the IP address of 66.46.21.12 in the call setup, it translates it to 192.168.0.6 instead. For this to work in both directions, a reciprocal rule must be entered on MBG-B:

Destination address: 66.46.21.11
Translation address: 192.168.0.5

Now a two-way call is properly routable between the two servers.

Note: This feature is suitable only for small numbers of servers. For *N* servers, each server requires a list of *N*-1 translation rules. This becomes difficult to manage for larger values of N. An auto-population feature, leveraging the clustering support, is being investigated for a future release.

11.3 Streaming Addresses

The MBG server will automatically determine the correct IP addresses to which endpoints must send their (S)RTP, if the server has been put into a standard, supported configuration and the correct network profile for that configuration has been chosen. See Services for full details on the supported configurations.

However, sometimes it is necessary to override the default streaming addresses, typically due to a non-standard configuration. When the admin views the Network profiles (under the Configuration tab), the current network profile will be shown with an interface to apply the supported network profiles.

Arbitrary addresses can be entered by selecting the Custom profile, if the “canned” configurations are not suitable. These addresses are used during signaling to inform the endpoints where to send RTP. If they are incorrect, there will be audio problems (typically one-way audio or no audio).

DMZ Deployment Profile

When the MBG server is deployed in a DMZ (see Figure 3 on page 5), all endpoints should send RTP to the IP address seen by the Mitel AMC during a sync operation. This is the MBG server's publicly-visible address after any NAT by the DMZ firewall. This address is configured automatically when DMZ mode is selected.

If this address is incorrect for some reason (such as multiple layers of NAT), use the Custom profile to enter the correct address.

Gateway Deployment Profile

A standard example of the gateway deployment is shown in Figure 2 on page 4. In this configuration, the WAN interface on the server is routable on the “public” network. This is referred to as the “set-side” streaming address, to which teleworker devices and service provider trunk equipment sends RTP. The “public” network is typically the Internet, but may instead be a managed service-provider network, MPLS LAN extension, corporate network, etc.

The LAN interface is attached to the private network. This is referred to as the “ICP-side” streaming address, to which LAN devices (phones), conference bridges, ICPs, voicemails, etc send RTP. The private and public addresses must be on different IP networks.

The defaults are usually acceptable. However, if not, they can be changed by using the Custom profile.

11.4 RTP Frame Size

By default, the RTP frame size is auto-negotiated between the endpoints. A size of 20 ms is common in North America, with 40 ms becoming common in Europe. If needed, the administrator can force use of a particular frame size. For example, some SIP trunk service providers insist on a particular RTP frame size.

The Configuration tab holds the global master setting. This setting is used as the default, and should be left on “Automatic” unless there is a pressing need to change it. Overrides can be placed on specific devices and trunks as required. For example, certain wireless networks handle RTP streams using larger (e.g. 40 ms) packets better than streams using smaller ones.

Note: The **f**rame size override only affects the streams to and from devices. The ICP-side streaming is always auto-negotiated. On SIP trunks, both WAN and ICP sides can be specified separately.

11.5 TFTP Block Size

MiNet devices use the TFTP protocol to fetch their firmware from the MBG server. The Mitel TFTP server is slightly non-standard – it uses symmetric UDP to traverse NAT devices, and a “sliding window” to improve performance – but is otherwise RFC-compliant.

The default block size in the TFTP protocol is 512 bytes, and with large firmware loads in a lock-step protocol like TFTP[4] this can take a prohibitively long amount of time to download. MBG employs the TFTP “blksize” option to attempt to transfer 4096 byte blocks, if possible. Depending on one’s network this may or may not be possible: the large packets will require fragmentation on a standard Ethernet network with a 1500 byte MTU, and some ISPs do not permit this.

Set the global TFTP block size to the largest value that works. Only the options in the pulldown (512, 1024, 2048 or 4096) are permitted.

11.6 Set-side Codec

MBG allows transcoding from G.711 to G.729 or from G.729 to G.711, if Compression licenses have been purchased. The usual use of this is to force a lower-bandwidth codec for remote devices. However, it can also be used to force G.711 for devices that do not support G.729 (e.g. voicemail systems) and that register to MCD as a MiNet IP device.

The global default setting is found under Configuration; Settings; MiNet Options, but the codec can also be set for each individual device.

11.7 SRTP Port Range

Each active call on the MBG requires two UDP ports for the RTP stream. Some SIP calls (video, T.38) may require four or more ports. (Two ports per SDP media line are required.) Ports are only used while calls are actually active, and are released upon the end of the call, or, for MiNet, end of the stream (which may be a hold or transfer, not actually the end of the “call”).

The default SRTP port range of 20000-31000 provides enough ports for over 5000 simultaneous voice calls or 2500 video calls. For smaller sites, this range can be reduced if desired. However, be sure any third-party firewalls have the matching range programmed. Mismatches between a DMZ firewall and the MBG will result in some calls having no audio (or one-way audio). This problem appears after many successful calls and is cleared by a reset of the MBG.

11.8 DSCP

MBG allows configuration of a Differentiated Services Code Point (DSCP) to be inserted into the header of ip packets. A separate value can be configured for signaliing and media packets. This is one of the tools available to help improve voice quality in some congested managed network environments.

As an example, consider a deployment with a managed WAN on the icp side of MBG and the Internet on the sets side of MBG. Now consider a situation where a managed WAN Service Level Agreement (SLA) is purchased that divides traffic into classes, including an Expedited Forwarding (EF) queue with priority over other traffic classes. In this situation, MBG can be configured to insert an EF value (46 decimal) for voice packets as they pass from the Internet to the icp side so that they can be protected on the managed WAN during periods of

4 Receipt of each block must be acknowledged before the next block is sent

congestion.

If the remote VoIP devices are only using voice then the bandwidth purchased for the EF queue must be large enough to accommodate the total number of concurrent voice streams passing through the MBG from Internet to managed WAN. However, if the remote VoIP devices will also be using video in this example, then the bandwidth purchased for the EF queue must account for both voice and video, keeping in mind that a video call requires 10 to 20 times more bandwidth than a compressed audio call even when devices are configured with the lowest bandwidth settings. Refer to section 12.3 Determine Bandwidth Requirements for guidance on calculating required bandwidth.

Alternatively, if the cost is prohibitive for provisioning enough EF queue bandwidth to support both voice and video needed for the deployment, then MBG should not be configured to insert an EF value (46 decimal) for voice/video packets. The reason for this is to prevent video passing through the MBG from impacting voice on a managed WAN where EF bandwidth has only been provisioned for voice. A future release of MBG will support configuring different values for voice and video to address this scenario.

Recommended settings when enough EF queue bandwidth has been provisioned to support both voice and video:

- voice/video : 46 decimal (Expedited Forwarding)
- signaling : 24 decimal (Class Selector 3)

Recommended settings when enough EF queue bandwidth has been provisioned to support voice only:

- voice/video : 34 decimal (Assured Forwarding 41)
- signaling : 24 decimal (Class Selector 3)

12 Sizing Your Installation

MBG installations come in many sizes, from a handful of remote workers, to large call centers with recording requirements, to service providers with hundreds of SIP trunks routed to customer vMCDs. This section provides guidelines for selecting appropriate hardware and network capacity for any size of installation.

For site with fewer than 500 users and 100 simultaneous streams, skip to section 12.2 Determine Call Equivalents.

Note: The calculations in this section assume that no other applications besides MBG will be running on the MSL server.

12.1 Determining Line Size for Large Sites

Step One: Determine Call Rate

The first step is to estimate how busy the site will be. Ideally, this figure will come from observations of actual usage, but it can be estimated. The services provided by the MBG server affect how much load it needs to handle.

Consider a typical teleworker scenario: 20 users working in a remote office. Assume that these users are on the phone about 10 minutes of each hour, or 6 CCS. If the users make two calls per hour, each call is 300s (5 minutes) long.

Multiply the average CPH rate by the total number of users to get the Erlang-B lambda value:

λ = 2 CPH * 20 users = 40 CPH

A call center might have usage of 20 CCS per agent. Assume an average call time of 600s (10 minutes). If the agent is busy 2000 call-seconds (20 CCS) and each call is 600s, the agent is handling 3⅓ calls per hour. For a busy call center with 1000 agents, lambda is:

λ = 3.3333 CPH * 1000 users = 3333.3 CPH

Step Two: Determine Service Rate

The *service rate,* represented by μ, is the mean number of calls the MBG can handle successfully per unit of time, without blocking. If it takes 20 minutes to service one call, then three calls can be serviced per hour, and the service rate is 3 CPH.

In the teleworker example above, the call duration is 300s, so MBG is processing 12 calls per hour:

μ = 12

In the call center example, the call duration is 600s, so the MBG is processing 6 calls per hour:

μ = 6

Step Three: Determine Grade of Service

The *grade of service*, represented by *P(b)*, is the percentage of calls that are turned away (blocked) because of insufficient capacity. The nominal and recommended P(b) is 1%, or 0.01.

Step Four: Erlang-B Calculator

An Erlang-B calculator can now be used with the values above to find the number of lines required to handle the load. (Free Erlang-B calculators are widely available online.) Following the teleworker example above, the Erlang-B calculation is:

λ = 40, μ = 12, P(b) = 0.01

c = 9

The site will need 9 lines to handle the load. In MBG terms, this is 9 simultaneous calls. The number of simultaneous calls is the key value in determining MBG resource requirements.

For the call center example:

λ = 3333.3, μ = 6, P(b) = 0.01

c = 583

The call center would require 583 lines (and agents) to handle the call volume. Again, this is 583 simultaneous calls going through the MBG.

12.2 Determine Call Equivalents

The next step is to determine the impact of transcoding, taps, and codec choices on CPU load and network bandwidth. The baseline is a single non-transcoded call with one RTP stream. The procedure in this step applies a load factor to convert more complex calls into an equivalent number of simple calls.

Usage	Call Equivalent (CPU)
Basic (non-transcoded) call	1
Transcoded call	2.5
SIP trunk call	1
Tapped call	1.5

Example:

4 MiNet sets all in calls with other parties, plus 2 SIP trunk calls, and two of the calls being tapped, all using G.711, would constitute:

CPU use = (4 MiNet calls – 2 tapped) + 2 SIP trunk + 2 tapped
= 2 untapped + 2 trunk + 2 tapped
= 2 + 2 + 2*1.5
= 7 calls

12.3 Determine Bandwidth Requirements

VoIP devices, including phones and SIP trunks, use RTP/SRTP for voice communication. The bandwidth required for the RTP stream depends on the codec selected by the device. Mitel Border Gateway supports the use of G.711, G.729, and G.722.1. Typically, there will be other requirements for Internet access, and these requirements (such as e-mail, web browsing, e-commerce) must be considered as well.

Failure to provide sufficient bandwidth for all Internet activities may compromise the quality of service of the Mitel Border Gateway.

The bandwidth figures for a single device are provided in *Bandwidth Requirements for the Remote Site* on page 19. For multiple devices, follow the procedure below.

Assumptions:

- Internet Service Providers specify bandwidth available to the user. i.e. PPPoE overhead does not need to be included in the provisioning of DSL bandwidth, but IP overhead does need to be included.
- RTP Bandwidth Requirements are as follows:
  - G.711 = 80 Kbps
  - G.729 = 24 Kbps
  - G.722.1 = 48 Kbps
- At 6 calls per hour Control stream bandwidth requirement is 20 Kbps peak for each 12 remote devices, and 1 Kbps idle for each remote device.
- The calculation below does not include bandwidth required for features such as paging. If group paging is enabled for teleworkers, an additional RTP stream should be provisioned for each remote member of the paging group.
- Whenever possible, transcoding should be performed by the ICP rather than the Mitel Border Gateway, as this typically provides improved voice quality.

If the mix of codecs in use cannot be reliably estimated, it is safest to assume G.711 for all calls.

Note: The actual bandwidth available will likely be less than the amount of bandwidth the ISP advertises. Also, the amount of available bandwidth may fluctuate throughout the day based on usage patterns of other subscribers.

The best way to determine the amount of available bandwidth is to use a speed test tool, preferably one provided by a third party rather than the ISP themselves – buyer beware.

G.711 Calculation

Bandwidth = number of users * idle control stream requirement
+ number of calls * RTP requirement
+ number of users / 12 * peak control stream bandwidth

For the teleworker example of 20 remote users:

20 * 1 Kbps + 9 * 80 Kbps + 20/12 * 20 Kbps
= 773 Kbps

For the call center example of 1000 remote agents:

1000 * 1 Kbps + 583 * 80 Kbps + 1000/12 * 20 Kbps
= 49307 Kbps or 48.15 Mbps

G.729a Calculation

Bandwidth = number of users * idle control stream requirement
+ number of calls * RTP requirement
+ number of users / 12 * peak control stream bandwidth

For the teleworker example:

20 * 1 Kbps + 9 * 24 Kbps + 20/12 * 20 Kbps
= 270 Kbps

For the call center example:

1000 * 1 Kbps + 583 * 24 Kbps + 1000/12 * 20 Kbps

= 16659 Kbps or 16.27 Mbps

Video Calculation

Some VoIP devices support video as well as voice, and extra bandwidth must be provisioned if video calls will be made. Although the exact bandwidth required depends on the content of the image, number of frames per second (fps), the codec and compression selected, and the video resolution, the list below gives approximations for some typical video streams.

Codec	Resolution	FPS	Bandwidth
H.263 or H.264	QCIF (176x144)	15	~ 128 kbps
		30	~ 256 kbps
	CIF (352x288) or QVGA (320x240)	15	~ 384 kbps
		30	~ 768 kbps
MPEG-4	CIF (352x288) or 320x240	15 – 30	~ 128 – 360 kbps

This list shows the bandwidth required for video streams from some Mitel devices contrasted with bandwidth required for other types of media streams.

Voice	If compression (G.729a) enabled: **24** Kbps (bi-directional) If compression not enabled (G.711): **80** Kbps (bi-directional)
MCA Collaboration	**192** Kbps (bi-directional)
UCA Video	**256** Kbps – **1600** Kbps (bi-directional)
UC360 Video	**512** Kbps – **1500** Kbps (bi-directional)

Note: A video call requires 10 to 20 times more bandwidth than a compressed audio call even when configured with the lowest bandwidth settings.

The Internet bandwidth provisioned at the MBG server must take into account the maximum number of simultaneous video calls from the remote devices and applications.

When a UC360 initiates a video conference it will also serve as the video bridge for the conference. For example, a UC360 that is acting as a video bridge for a 4 party conference will require three times the video bandwidth and three times the audio bandwidth required by a UC360 that is only a participant in the conference.

Video calls between UCA 6.0 and UC360 2.0 are supported through MBG but they do not negotiate bandwidth at the time of writing. For example, a UCA client on the Internet will receive video at the rate configured on a UC360 on the LAN even if the UCA is configured to use low bandwidth. This will be rectified in a future release of UCA and/or UC 360.

MCA voice and video conferencing between MCA clients via the MCA server is also supported through MBG. The bandwidth usage per video stream is configurable on the MCA client. An additional consideration is that an MCA client can receive multiple video streams, one for each video participant in the conference. That number can be reduced at the MCA client by minimizing or closing video windows.

For details and current values, please see the engineering guidelines for the devices/applications referenced as examples here *(*available from http://edocs.mitel.com/).

Fax Calculation

A fax call made over a SIP trunk or to a SIP device supporting fax will be either a G.711 voice stream or a T.38 fax session. For the purposes of bandwidth calculations, consider both cases to be an 80 kbps G.711 stream.

Call Recording Calculation

When using MBG's Secure Call Recording service, a third-party Call Recording Equipment (CRE) device registers to MBG and requests “taps” of calls in progress. The control connection is an SSL-encrypted TCP stream authenticated by an X.509 client certificate provided by the CRE. (Refer to the *MBG Installation and Maintenance Guide* for information on the process used to obtain and install the CRE certificate.)

A small amount of bandwidth is used for the CRE control connection. However, it is usually insignificant when compared to the volume of voice traffic, and can be safely ignored. A small amount of CPU load is also incurred for the control connection. Again, it is usually insignificant compared to the load of processing voice signaling and RTP.

MBG makes a copy of the RTP streams for each call that is being recorded, and forwards them to the CRE. Therefore, each tapped call requires 50% more bandwidth than an untapped call. Only audio is recorded; any video or T.38 streams should be ignored when calculating call recording bandwidth requirements. Simply estimate the number of calls that will be recorded simultaneously, and multiply by the codec in use. When in doubt, it is safest to assume G.711 for all calls.

For example, assume that 10 calls will be recorded at a time. All calls are G.711.

Bandwidth = 10 calls * 80 kbps

= 800 kbps

The site requires 800 kbps on top of the bandwidth used by the calls themselves.

Note: When transcoding, the bandwidth requirements are different on the two “sides” of the MBG.

Example Bandwidth Calculation

A site has 48 SIP trunks shared by remote and in-office users. Most users are in the office, but 100 work in various remote branch offices with Teleworker phones hosted on an MCD at the main office. Remote phones are configured for G.729 to save bandwidth, and all SIP trunk calls are G.711. (MCD handles any transcoding.) In addition, the site records up to 10 remote office calls at any given time.

At peak, the site uses 40 trunk channels and 75 of the remote users are in a call. Ten percent of the remote users are in UCA video calls configured to match the lowest bandwidth setting of a UC360 device.

The system is deployed in gateway mode, in parallel with the company firewall.

Step one: G.711 trunk calls

WAN BW = 40 channels * 80 kbps
= 3200 kbps
LAN BW = 40 channels * 80 kbps
= 3200 kbps

Step two: Remote office calls; voice

WAN BW = 75 * 24 kbps
= 1800 kbps
LAN BW = 75 * 24 kbps
= 1800 kbps

Step three: Remote office calls; video

10% of 75 users = 7.5
WAN BW = 7.5 * 512 kbps
= 3840 kbps
LAN BW = 7.5 * 512 kbps
= 3840 kbps

Step four: Recorded calls

LAN BW = 10 tapped calls * 24 kbps
= 240 kbps

Step five: Totals

Adding up the results from the four steps, the WAN bandwidth requirement is 3200 + 1800 + 3840 kbps for a total of 8840 kbps. The site will require at least a 9 megabit connection just for voice and video capacity. The LAN bandwidth, which includes tapped calls, is 3200 + 1800 + 3840 + 240, or 9080 kbps.

Note: For a server in LAN mode or in a DMZ (with a single NIC), calculate the bandwidth required for the WAN "side" (no tap streams) and LAN "side" (including tap streams) and add them together, since one NIC handles all of the traffic. In the example above, the network would have to handle 8840 + 9080 = 17920 kbps, or 17.9 Mbps. However, the WAN pipe still only has to handle 9 Mbps.

Note: See also sections 12.6, 12.7, and 12.8.

12.4 Hardware Selection

Installations with less than or equal to 500 users and up to 100 simultaneous streams can select *any server on the **MSL Qualified Hardware List***. Larger sites can use the Call Equivalents obtained in section 12.2 Determine Call Equivalents and the information below to determine the necessary number of servers.

12.5 Performance Characteristics and Limits

Mitel continually evaluates hardware and virtual hardware platforms with MBG to determine its maximum capacity. The following are the results of testing with MBG 8.0. These numbers assume a typical office call rate of 6 CCS.

Physical Hardware

CPUs: 2 x Intel Xeon E5620 (Nehalem quad core), 2.4 GHz, with HyperThreading
Memory: 24 GB
Network: Gigabit Ethernet
OS: Mitel Standard Linux

Capacity:

- 5000 registered devices
- 1750 simultaneous G.711 “simple calls” [5]

VMWare Virtual Hardware

Host CPUs: 2 x Intel Xeon E5620 (Nehalem quad core), 2.4 GHz, with HyperThreading
Host Memory: 24 GB
Host Network: Gigabit Ethernet
OS: VMWare vSphere 5.0 [6]

Two configurations were tested: vMBG “small business” and vMBG “enterprise”.

Capacity - “small business” configuration:

- 16 vMBGs – 1 vCPU each
  - 150 registered devices (each vMBG)
  - 30 simultaneous G.711 “simple calls” (each vMBG)[5]

Capacity - “enterprise” configuration:

- 2 vMBGs – 3 vCPUs each
  - 2500 registered devices (each vMBG)
  - 500 simultaneous G.711 “simple calls” (each vMBG)[5]

12.6 Web Proxy and Remote Management Service Requirements

The bandwidth requirements for any and all applications proxied by Web Proxy and Remote Management Service are documented in their respective Engineering Guidelines, and are beyond the scope of this document. See 7.3 Web Proxy for relevant firewall rules.

12.7 UCA and MCA Requirements

UCA with Softphone module counts as a remote IP set, with additional bandwidth required for its login and presence. The login and presence connections use negligible bandwidth and do not require real-time priority. The UCA SIP Softphone supports video calls, which requires 10 to 20 times more bandwidth than a compressed audio call even when configured with the lowest bandwidth settings (see section 12.3 for examples).

MCA conferencing with video between MCA clients via the MCA server is also supported through MBG, which requires significantly more bandwidth than audio calls (see section 12.3 for examples).

An MCA collaboration connection can also require considerable bandwidth, based on the features used, the number of presenters, and the number of participants. The table below provides a typical use-case by number of presenters and participants, with the estimated bandwidth required. For more details, refer to the MAS Engineering Guidelines.

Note: The table assumes the following settings
PowerPoint sharing: enabled
Desktop/App Sharing: disabled
Audio Setting: good
Video Setting: low

5 See section *12.2 Determine Call Equivalents*

6 MBG 8.0 supports vSphere 4.1, 5.0, and 5.1

The collaboration bandwidth is in addition to that required for voice communications. Refer to 7 Additional Application Requirements for the relevant firewall rules.

Presenters	Participants	Bandwidth Required
1	1	192 Kbps
1	2	256 Kbps
1	5	448 Kbps
2	2	460 Kbps
2	5	736 Kbps
1	10	768 Kbps
2	10	1.2 Mbps
2	50	4.9 Mbps
5	100	18.7 Mbps

Table 3: Bandwidth Requirements for MCA Collaboration

12.8 Mitel Contact Center Softphone Requirements

MBG release 4.5 introduced support for the Mitel Contact Center Softphone version 5.3. The softphone has multiple components. Bandwidth requirements of the voice component are identical to any other Mitel set using G.711 or G.729 (compression). In addition to voice, Mitel Contact Center Softphone supports the following connections through the MBG server:

MBG Server Port Used	Default Destination Port	Description
TCP 36000	TCP 80	HTTP authentication and user profile access
TCP 36001	TCP 443	HTTPS authentication and user profile access
TCP 36002	TCP 5024	Real-time client
TCP 36003	TCP 5025	Auditor connection
TCP 36004	TCP 5026	Telephony proxy

The “MBG Server Port Used” column indicates the port on which MBG listens, on its Internet-facing side, for the incoming connection. The “Default Destination Port” is the port on the Contact Center server to which MBG routes the connection. Additional Mitel contact center connections were added over multiple releases and as of MBG 8.0 also includes MBG Server TCP ports 35001 to 35008 inclusive. Refer to *7.2 Mitel Contact Center* on page 28 for firewall configuration instructions.

Bandwidth requirements will vary depending on the type of activity being performed. During installation of the client, software is downloaded and installed. The client periodically checks for updates and may download and install them. The bandwidth required by these tasks is not included in the tables below; it is assumed to be part of the bandwidth used by the user's PC.

When a user first launches the Contact Center client and selects devices to view, there is a database transfer. The size of the database depends on the objects selected, as follows:

1 Queue (Q) = 65 KB
1 Agent (A) = 39 KB
1 Employee = 20 KB

1 Extension = 17 KB
1 Network Monitor (NM) (1 x MCD) = 56 KB

Refer to the following table to determine the size and download time for the database at various line speeds.

# of Devices	Config	Data Size	512 Kbps	1024 Kbps	1.54 Mbps	2.048 Mbps	10 Mbps
5	1Q, 1A 1Ex, 1Em, 1NM	157.6 KB	00:00:02	00:00:01	00:00:01	00:00:00	00:00:00
50	15Q, 11A, 11Ex, 12Em, 2NM	303.2 KB	00:00:04	00:00:02	00:00:01	00:00:01	00:00:00
100	25Q, 25A, 22Ex, 25Em, 3NM	348.8 KB	00:00:06	00:00:03	00:00:02	00:00:01	00:00:00
500	200Q, 100A, 92Ex, 100Em, 8NM	1.304 MB	00:00:20	00:00:10	00:00:06	00:00:05	00:00:01
1500	500Q, 300A, 385Ex 300Em 15NM	3.528 MB	00:00:55	00:00:27	00:00:18	00:00:13	00:00:02
5000	2086Q, 2379A, 247Ex, 322Em, 16NM	14.24 MB	00:03:42	00:01:51	00:01:13	00:00:55	00:00:11
8100	3036Q, 4379A, 247Ex, 322Em, 16NM	22.72 MB	00:05:55	00:02:57	00:01:57	00:01:28	00:00:18

Note: Note: The use of traffic shaping (to prioritize RTP ahead of other packets) could be used to prevent data transfers, such as the initial DB transfer above, from affecting calls in progress.

The table below provides bandwidth requirements for a typical contact center configuration at various call rates, in addition to the bandwidth required for voice communications.

Calls per Hour (CPH)	Bandwidth per ICP	Bandwidth per Real-Time Client
100	0.48 kbps	0.48 kbps
1000	4.88 kbps	4.72 kbps
2000	9.76 kbps	9.44 kbps
3000	14.72 kbps	14.16 kbps
4000	19.6 kbps	18.88 kbps
5000	24.48 kbps	23.6 kbps
6000	29.36 kbps	28.32 kbps

Note: This is a guideline only. Actual results may differ depending on the contact center configuration.

13 Virtual MBG Considerations

Virtual Mitel Border Gateway (vMBG) is the MBG software and supported Mitel Standard Linux (MSL) operating system bundled in a VMware Virtual appliance, to run in the VMware vSphere/ESX(i) hypervisor. The software is packaged in Open Virtualization Format (OVF) for deployment into a VMware environment. Refer to the virtualization sections of the MAS engineering guidelines for details and current best practices.

13.1 Licensing

The standard MBG base kit cannot be used to run an instance of vMBG. The “Mitel Border Gateway Virtual Appliance” base kit (part number 54005339) must be used instead. An existing base kit can be converted.

Warning: If the wrong base kit is used, the vMBG will have no licenses.

13.2 Upgrades

A virtual MBG can be upgraded just like a physical MBG, by visiting the MSL Blades panel and downloading the update from the Mitel AMC. Alternately, an MBG CD, available from Mitel OnLine, can also be used via the VMware console.

MSL can also be upgraded either with the MSL ISO image available from Mitel OnLine, or by clicking on the ServiceLink blade upgrade in the MSL Blades panel.

From time to time, Mitel releases new OVA files on Mitel OnLine. The OVA must be used for initial deployment of a vMBG, but can also be used for upgrades by following the procedure below:

- Back up[7] the current MBG using the application's back-up button
- Deploy the new OVA
- Restore the backup file using the application's restore button

This procedure can also be used to convert a physical to a virtual MBG.

Alternately, a full backup of the MSL server can be performed, followed by deploying a new OVA, and then a restore of the backup using the MSL server console.

13.3 Host Server Requirements

Hardware

The recommended minimum hardware to run vMBG on VMware vSphere/ESX(i) is:

- 2 x Intel Xeon E5620 (Nehalem quad core), 2.4 GHz, with HyperThreading
- 24 GB RAM
- 300 GB disk allocated to storage pool

See *12.5 Performance Characteristics and Limits* on page 45 for more information on server capacities.

7 Mitel recommends making frequent backups of your important data

Software

Virtual MBG is supported on the following platforms:

- VMWare vSphere 4.1, 5.0, 5.1 (ESX/ESXi 4.1, 5.0, 5.1)

The following standard features of vSphere are not currently supported for vMBG:

- **Update Manager Server & OS Patching:** This feature does not support MSL and cannot be used. MSL updates should be installed via the Blades panel or an MSL CD.
- **VMSafe**
- **vCenter Converter**

Use of the following features is **not recommended**:

- **Power off:** This is equivalent to pulling the power on a physical server, and could result in data corruption on the virtual disk. Use the MSL Shutdown command to halt the vMBG.
- **Snapshot while powered-on:** The VM snapshot functionality creates considerable disk I/O load. Use of this feature can substantially degrade the voice quality of calls in progress.

Finally, the following vSphere features require special consideration.

- **Deployment:** When vMBG is deployed, the vSphere client may change the network adapters from VmxNet3 to VmxNet. This results in a lack of network connectivity in the VM. If this happens, the network adapters must be manually updated using the vSphere client, by deleting the existing adapters and creating new ones of type VmxNet3.
- **Export:** Exporting the virtual appliance changes some of the licensing input values, resulting in invalid licenses. The solution is to clear the server's hardware footprint at the AMC and re-register it.
- **Cloning while powered-off:** This is supported, but a new AMC Application Record ID will be required for the cloned virtual machine.
- **Snapshot while powered-off:** Using a snapshot to create a restore point before a major upgrade is recommended. However, to avoid performance issues afterwards, Mitel recommends deleting the snapshot after confirming that the upgrade was successful and has caused no issues.
- **VMotion:** During the actual vMotion period (typically from 30 seconds to two minutes[8]), certain communication services may become temporarily unavailable and some temporary degradation of voice quality may occur.
- **SRM:** Site Recovery Manager is a powerful and sophisticated Vmware virtual infrastructure management application. Integration of Mitel virtual appliances within SRM requires Mitel Professional Services to assist with customer-specific configuration, including the deployment of Mitel-specific automated scripts that assist in communications service restoration at the recovery site.

13.4 High-Availability

As with physical MBG servers, high-availability is achieved through MBG clustering. However, with virtual hardware, there is an additional consideration. To avoid a single point of failure, Mitel recommends using VMWare anti-affinity rules to prevent all cluster nodes from running on the same physical host hardware.

8 Actual vMotion duration depends on site-specific attributes

14 Solutions To Common Problems

14.1 Changing a Cluster Node's IP Address

MBG clustering uses IP addresses to identify each node and to initiate cluster communications connections.

To change a node's IP address, Mitel recommends the following procedure:

1. Make sure that the node to be changed is not the master node. Take ownership from another node if required.
2. From the slave node to be changed, go to the clustering tab and click on the “Leave cluster” button.
3. Reconfigure the address via the MSL console, and follow the prompts to reboot.
4. Join the server to the cluster.

14.2 T.38 Faxing Does Not Work With NAT

Use of T.38 fax is not compatible with NAT. A fax device behind a NAT firewall/router that does not perform its own NAT traversal may not be able to receive T.38 faxes. It may be able to send them.

During the T.38 setup, the receiving fax listens for incoming tones from the sending fax (no-signal, v21-preamble, etc), then sends tones in response. However, MBG cannot send media to a device behind NAT until that device first sends at least one media packet to the MBG. In a T.38 setup, that will never happen, and the sender's tones are discarded. The call fails (after several retries by the sender).

If the sending fax is behind NAT and the receiving fax is not, the call should work.

It is possible to receive T.38 faxes when behind NAT with certain types of call setup. However, it is not wise to rely on a certain type of negotiation since T.38 calls can be set up in several ways.

Fax devices that support NAT traversal such as STUN should be able to work around this limitation. They appear to MBG as a device with a public address, and MBG can send to them without needing to receive a packet first. Use of G.711 faxing is another option, although it requires a very clean stream. Customers can also use a third-party fax to email or fax to web service.

Note: This problem does not apply to SIP trunks; there is no NAT on trunks.

15 Appendix A: Firewall Configuration Reference

The information in this section is provided to allow configuration of a customer's firewall for the Mitel Border Gateway in DMZ deployment. This configuration is automatic in the "MBG server as the gateway" deployment. In all cases below, "server" refers to the Mitel Border Gateway server (that is, the MSL server). In the Direction column, the direction of the arrow indicates permission to initiate new connections in that direction. These rules assume a firewall that will permit return traffic on an existing established connection.

Port Range	Direction	Purpose and Description
TCP 22 (SSH)	Server -> Internet	AMC Communications. Allow outbound packets (and replies) on TCP port 22 between the MBG Server and the Internet to enable server registration, software and license key downloads, alerts, and reporting.
TCP 22 (SSH)	Internet -> Server	Remote SSH access (Optional). If the admin wishes to administer the MBG server remotely via the command line over the Internet, this rule is required.
TCP 22 (SSH)	LAN -> Server	Remote SSH access (Optional). If the admin wishes to administer the MBG server remotely via the command line from the LAN, this rule is required.
UDP 53 (DNS)	Server -> Internet	DNS. The server requires DNS to look up the IP address of the Mitel AMC and for correct operation of SIP. Alternatively, the server can be configured to forward all DNS requests to another DNS server. See the MSL Installation and Administration Guide for details.
TCP 443 (HTTPS)	Internet -> Server	Remote Server Management (Optional). Allow inbound and outbound packets on TCP port 443 between the MBG server and the Internet to allow remote management of the server, if required. HTTPS access to the manager on the external interface must also be explicitly enabled from the server manager interface. The firewall should be configured to limit HTTPS access to desired manage- ment hosts.
TCP 443 (HTTPS)	Internet -> Server	Web Proxy client connections (Optional). If using the Web Proxy application, traffic must be permitted between the Internet and the proxy in the DMZ.
TCP 443 (HTTPS)	LAN -> Server	Local Server Management. Allow inbound and outbound packets on TCP port 443 between the MBG Server and the LAN to allow for management of the server. HTTPS access to the manager on the external interface must also be explicitly enabled from the server-manager interface. The firewall should be configured to limit HTTPS access to desired management hosts.
UDP 20000 to configured upper bound in Advanced tab (SRTP)	Internet -> Server LAN -> Server	Voice Communications. Allow incoming SRTP on UDP ports 20000 to the configured upper bound from all streaming devices on the LAN and the Internet. Misconfiguration here is a common cause of one-way audio problems. Note that as of release 7.0, MBG defaults to using even-numbered ports for RTP, leaving the odd-numbered ports for RTCP. The Internet portion of this rule can be safely omitted in the absence of Internet traffic.

UDP 1024 - 65535 (RTP)	Server -> LAN Server -> Internet	Voice Communications. Allow outgoing SRTP on UDP ports greater than, or equal to 1024 from the server to all streaming devices on the LAN and the Internet. Misconfiguration here is a common cause of one-way audio problems. Note that as of release 7.0, MBG defaults to using even-numbered ports for RTP, leaving the odd-numbered ports for RTCP. The Internet portion of this rule can be safely omitted in the absence of Internet traffic.
TCP 443 (HTTPS)	Server -> LAN	Web Proxy client connections (Optional). If using the Web Proxy application, traffic must be permitted to and from the LAN to the proxy on the DMZ.
TCP 443 (HTTPS)	Internet -> Firewall	ConnectionPoint traffic (Optional). To support AWC through the Web Proxy, a second, dedicated IP address is required for the ConnectionPoint traffic. This traffic will arrive on TCP port 443 and must be forwarded to the Proxy at the port configured in the Proxy interface to handle it. The Proxy will then forward this traffic to port 4443 on the LAN.
TCP ?	Firewall -> Server	ConnectionPoint traffic (Optional). If using AWC through the Web Proxy, traffic from the Internet to each port configured to receive Connection- Point traffic in the Web Proxy must be permitted.
TCP 4443	Server -> LAN	ConnectionPoint traffic (Optional). If using AWC through the Web Proxy, traffic to this destination port must be permitted between the proxy on the DMZ and the server on the LAN.
TCP 80	Internet -> Server LAN -> Server	Certificate Management (Optional). On any server hosting clients that make use of MiSSLTunnel with a client certificate (UCA, CIS, etc), this port must be open to the Internet to permit the web service to submit a certificate signing request (CSR), check on the status of that request, and download the certificate. Also needed for CREs to register with SRC control interface.
TCP 443	Server -> LAN	UC Advanced Support (Optional). If making use of the UC Advanced support, and the ability to remotely access NuPoint voicemail is required, this port must be permitted from the Server to the LAN IP of the NuPoint server.
TCP 36005	Internet -> Server	UC Advanced Support (Optional). If making use of the UC Advanced support, this port must be permitted from the Internet to the Server. This port permits a SOAP web service from UCA to a server on the LAN.
TCP 36006	Internet -> Server	UC Advanced Support. To permit the UCA client to connect and retrieve NuPoint voicemail, this port must be permitted.
TCP 36007	Internet -> Server	UC Advanced Support. To permit the UCA client to connect to the UCA server via SIP over TLS, this port must be permitted.
TCP 36008	Internet -> Server Server -> LAN	UC Advanced Support. To permit the UCA client to connect to the UCA server for presence information, this port must be permitted.
TCP 37000	Server <-> LAN Internet -> Server	UC Advanced Support. To permit the UCA client to connect to the collaboration server on the LAN side, this port must be permitted. Failure to do so will result in the collaboration features failing to function.

TCP 80	Server -> LAN	UC Advanced Support (Optional). If making use of the UC Advanced support, this port must be permitted from the Server to the LAN IP of the UCA server, and also to any NuPoint servers. Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 5060	Server -> LAN	UC Advanced Support (Optional). If the ability to use SIP over TCP is needed, this port must be permitted from the Server to the UCA server on the LAN.
TCP 36000	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 36003	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 5025	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 36001	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 443	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 36002	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 5024	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 36004	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 5026	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35001	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 5030	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35002	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.

TCP 7001	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35003	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 7003	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35004	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 8083	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35005	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 8084	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35006	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 42440	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 35007	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 1433	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 6810	LAN -> Server	Call recording support (Optional). To enable a third-party call recording equipment (CRE) server to connect to the SRC control interface on MBG, this port must be enabled.
TCP 6815	Server -> ICPs	Indirect Call Recording support (Optional). To enable MBG to connect to the Indirect Call Recording connector on MCDs which support it.
UDP 30000 to 40000	Server -> LAN	Voice Recording. For streaming voice streams from the MBG server to the CRE for recording purposes.
TCP 6809	Between servers in a cluster	Cluster Comms. If making use of clustering in MBG, this port must be open between the servers in the cluster to permit them to communicate with one another.

TCP 6800, 6801 and 6802	Server -> LAN Server -> ICP(s)	MiNet Call Control. Allow incoming and outgoing packets for TCP ports 6801 (MiNet-SSL) and 6802 (MiNet-Secure V1) between the server and the Internet. Allow incoming and outgoing packets for TCP ports 6800 (unencrypted MiNet), 6801 and 6802 between the server and the LAN and the server and the ICP(s). The LAN rule can be omitted if there are no IP sets on the LAN, but ensure that the ICP(s) can communicate with the server's public address.
TCP 6801 and 6802	Internet -> Server	MiNet Call Control. Same as above. Port 6800 should not be used on the Internet as it is unencrypted. Port 6802 is not required with an Enhanced Security deployment.
TCP 3998, 6881	Internet -> Server	SAC Connection Support. Allow incoming TCP from the Internet to the MBG server, on ports 3998 and 6880, to support applications and web browsing, respectively, on the 5235, 5330, 5340 and Navigator sets. There is an additional LAN rule that follows this to complete the support.
TCP 3998, 3999 and 6880	Server -> ICP(s)	SAC Connection Support. Allow bidirectional TCP traffic on port 3999 to/from the ICP(s). This is to support the applications on the 5235, 5330, 5340 and Navigator sets. Note: 3998 and 6880 require an additional, MBG server on the LAN to which the Internet-facing server is daisy-chained.
TCP 80	Server -> LAN Server -> Internet	SAC Connection Support (Optional). Allow TCP port 80 from the server to the Internet, and to the LAN, to support web browsing on the 5235, 5330, 5340 and Navigator sets. Also required to the Internet to allow browsing of the Internet from the set.
TCP 6806	Internet -> Server	IP Console Support (Optional).
TCP 1606	Server -> LAN	IP Console Support (Optional).
TCP 6807	Internet -> Server	IP Console Support (Optional).
TCP 443	Server -> LAN	IP Console Support (Optional).
UDP Port 20001	Server -> ICPs	HTML application autopopulation support (Optional). To permit MBG to autopopulate HTML applications from the ICPs, bidirectional traffic from a random UDP port on MBG to UDP port 20001 on the ICPs must be permitted.
UDP 5060	Server <-> LAN Server <-> Internet	SIP Support. If the SIP connector is enabled, then this port is required for SIP signaling between MBG and the set, and MBG and the ICP, and for SIP trunking support.
UDP 5064	Server <-> LAN Server <-> Internet	Legacy SIP Trunk Support (Optional). This connector is deprecated and should no longer be used. All SIP should be handled via UDP port 5060.
TCP 5060	Server <-> Internet	UCA SIP TCP Support (Optional). If SIP UDP is enabled and UCA is enabled then a tcp-udp bridge connector will be enabled. This port is required for SIP signaling over TCP between MBG and UCA clients that have been configured for TCP.
TCP 5061	Server <-> Internet	UCA SIP TLS Support (Optional). If SIP UDP is enabled and UCA is enabled then a tls-udp bridge connector will be enabled. This port is required for SIP signaling over TLS between MBG and UCA clients that have been configured for TLS.
TCP 5269	Server <-> LAN Internet <-> Server	UC Advanced Support. To permit the UCA server to connect to another UCA server using the XMPP protocol. Failure to do so will result in the federation features failing to function.

TCP 35008	Internet -> Server	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the Internet to the server.
TCP 8188	Server -> LAN	Contact Center Support (Optional). To enable use of the prairieFyre Contact Center solution, this port must be permitted from the server to the Contact Center server on the LAN.
TCP 21	Internet -> Server	MCD Remote Upgrade (Optional). To permit MCD software to be uploaded to the MBG server (FTP passive mode).
TCP >1023	Internet -> Server	MCD Remote Upgrade (Optional). To permit MCD software to be uploaded to the MBG server (FTP passive mode).
TCP 21	Server -> LAN	MCD Remote Upgrade (Optional). To permit MCD software to be downloaded to the MCD (FTP passive mode).
TCP >1023	Server -> LAN	MCD Remote Upgrade (Optional). To permit MCD software to be downloaded to the MCD (FTP passive mode).

GLOSSARY

APC Application Processor Card

ATM Asynchronous Transport Mode. A switching protocol that uses asynchronous time-division multiplexing (TDM) to put data into fixed-size cells. It is suitable for carrying real-time payloads such as voice and video.

AWC Audio Web Conferencing (See *MCA*)

CCS Centum Call Seconds. A unit of measurement used in traffic and queuing theory calculations that is equal to 100 seconds of conversation. One hour of telephone traffic on one line is equal to 36 CCS, which is equal to one erlang (a more common measurement).

CPH Calls Per Hour

CRE Call Recording Equipment

CSR Certificate Signing Request

DHCP Dynamic Host Configuration Protocol (RFC 1541)

DMZ De-Militarized Zone. A portion of a network which is behind a firewall but has elements that are exposed to the Internet.

DSL Digital Subscriber Line

Erlang A unit of traffic density in a telecommunications system. One erlang is the equivalent of one call (including call attempts and holding time) in a specific channel for 3600 seconds in an hour. It is equal to one hour of conversation, or 36 CCS.

G.711 ITU-T codec audio standard, specifying an audio signal with a 3.4 KHz bandwidth (ordinary analog voice signal) over an A-law and μ-law digitized, linear PCM at 64Kbps. In G.711, encoded voice is already in the correct format for digital voice delivery in the PSTN or through PBXs.

G.729 This ITU-T standard describes CELP compression where voice is coded into 8-Kbps streams. The two variations of this standard (G.729A and G.729A Annex A) differ mainly in computational complexity; both provide speech quality similar to 32-Kbps ADPCM.

ICP IP Communications Platform

IETF Internet Engineering Task Force. The official specification documents of the Internet Protocol suite are defined by the Internet Engineering Task Force (IETF) and the Internet Engineering Steering Group (IESG). These specifications are recorded and published as standards track RFCs. (See *RFC*).

IP Internet Protocol (RFC 1122 Section 3.)

IPSec Internet Protocol Security

ISP	Internet Service Provider
MBG	Mitel Border Gateway
MCA	Mitel Collaboration Advanced, formerly known as AWC.
MCD	Mitel Communications Director, formerly known as the 3300 ICP.
MiNet	Mitel Network Layer Protocol. A signaling protocol used to transport messages between the PBX and all Mitel IP phones. MiNet is encapsulated in TCP.
MSL	Mitel Standard Linux. The standard Linux distribution used and maintained by Mitel as a platform for all applications
NAT	Network Address Translation. A technique for translating one set of IP addresses, often private, to another set, often public (RFC 1631)
PPP	Point-to-Point Protocol
PPPoA	Point to Point Protocol over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RFC	Request For Comments. A standards document for the public Internet. RFCs are produced by the IETF and its working groups, as well as other bodies, to define and ratify new Internet standards and changes to existing standards. RFCs must first be published as Internet Drafts.
RTP	Real-time Protocol (RFC 1889)
SIP	Session Initiation Protocol (RFC 3261 et al.)
SRC	Secure Recording Connector
SRTP	Secure Real Time Protocol (RFC 3711)
SSL	Secure Socket Layer
TCP	Transmission Control Protocol (RFC 1122)
TDM	Time-Division Multiplexing. A system of carrying multiple signals on one carrier by dividing the multiple inputs into fixed-length (time) samples, and placing them one after the other onto the carrier medium.
TFTP	Trivial File Transfer Protocol (RFC 783). A simple file transfer protocol (no password protection or user directory services) that uses UDP to transfer files across a network
UDP	User Datagram Protocol (RFC 1122)
VoIP	Voice over IP

VPN	Virtual Private Network
WP	Web Proxy

INDEX

3300....3, 15, 25
5000 CP....15, 25
Agent....47
AMC....17, 37, 49, 50, 52
AWC....53, 58, 59
bridged mode....4
Call Equivalent....41
Call Recording....2, 7-9, 14, 27
CCS....45
Certificate....53, 58
channel....20, 25
CIS....9, 53
cluster....4, 13, 26
clustering....4, 26, 33, 35-37
clusters....34
codec....38, 41
compression....20, 38, 43, 47
ConnectionPoint....29, 53
contact center....9, 28, 47, 48
CRE....10, 11, 25, 33-35, 50, 53, 55, 58
CSR....53, 58
daisy-chain....11-13, 56
DHCP....3, 4, 8, 18
DMZ....2, 5, 10-13, 15-17, 22, 23, 26-28, 35
DNS....6, 17, 23, 25, 26, 52
DSCP....31
dynamic IP....19
Extension....2, 37, 48
firmware....22
frame size....21, 37, 38
framesize....21, 37, 38
G.711....20, 21, 38, 41, 43, 47
G.729....20, 21, 38, 43, 47
HTB....31
HTML application....22, 56
HTML Applications....22
ICP....3, 7, 8, 11, 15, 22, 25, 26
licenses....7, 25
Local Streaming....27
Management....10, 13, 15, 36, 50, 52, 53
MAS....13, 14
MCA....20, 43
MCD....8, 10, 15, 22, 25
media stream....2, 25
MICD....6, 15
MiNet....2, 6, 7, 12, 14, 16, 18, 21, 22, 30
Mitel Communications Director....3, 15
Mitel Standard Linux....1, 3, 19, 30, 45, 49
Monitor....48
MSL....1, 3-5, 8, 15, 19, 31, 45, 49
NAT....3-6, 10, 15, 16, 18
NAT traversal....6, 10, 16
NuPoint....53, 54
one-way audio....16, 37, 38, 52, 53
Open Virtualization Format....49
Options Keepalives....23
OVF....49
PBX....2, 18
port-forwarding....2, 4, 6, 16
PPPoA....3, 4, 18, 19
PPPoE....3, 4, 18, 19
PPTP....19
Queue....31, 47
resiliency....11, 23, 25, 33, 36
RTCP....52, 53
RTP....16, 17, 21, 27, 30
SAC....22, 56
SDP....38
Secure Recording Connector....1, 2
Security....14, 19, 22, 30
silhouette....6, 15
SIP....2, 6, 10, 12, 14-16, 18, 20-23, 25, 26, 30, 35
SIP Trunk...2, 10, 14, 15, 25, 26, 31, 37, 38, 40, 41, 56
SIP trunks....2, 10, 25
softphone....9, 19
SRC....1, 27, 53, 55, 59
SRTP....27, 30, 36, 38, 52, 53, 59
SSH....15, 52
streaming....12, 27, 36-38, 52, 53, 55
T.38....38
Teleworker....2, 3, 7-9, 12, 18
TFTP....8, 18, 22, 38
Traffic Shaping....4
transcoding....38, 41, 44
trunk....2, 10, 25, 26
U....46
UCA....22, 28, 46, 53, 54
UDP flooding....16, 26
Unified Communicator Advanced....28
Video....27, 30, 38, 46
vMBG....46, 49
vMCD....15
VMware....46, 49
VPN....10, 19
Warning: Management....12
Web Proxy....13, 14, 29, 46, 52, 53, 60
weight....34, 35

zones.....33, 34
.....27
trunk.....41